

~~SECRET//ORCON,NOFORN~~

UNITED STATES

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

FOREIGN INTELLIGENCE SURVEILLANCE COURT APR 22 AM 11:03

WASHINGTON, D.C.

LEE ANN FLYNN HALL
CLERK OF COURT

UNDER SEAL

**GOVERNMENT'S EX PARTE SUBMISSION OF REAUTHORIZATION
CERTIFICATION AND RELATED PROCEDURES, EX PARTE SUBMISSION OF
AMENDED CERTIFICATIONS, AND REQUEST FOR AN ORDER APPROVING
SUCH CERTIFICATION AND AMENDED CERTIFICATIONS ~~(S)~~**

In accordance with subsection 702(g)(1)(A) of the Foreign Intelligence
Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and
through the undersigned Department of Justice attorney, hereby submits ex parte the
attached certification, DNI/AG 702(g) Certification [REDACTED] This certification
reauthorizes DNI/AG 702(g) Certification [REDACTED] which expires on [REDACTED] 2011.
Attached as Exhibits A, B, C, D, and E to DNI/AG 702(g) Certification [REDACTED] are the
targeting and minimization procedures to be used under the certification. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

Classified by:

~~Tashina Gauhar, Deputy Assistant Attorney
General, NSD, DOJ~~

Reason:

~~1.4 (c)~~

Declassify on:

~~18 April 2036~~

The National Security Agency (NSA) targeting procedures and Federal Bureau of Investigation (FBI) minimization procedures attached to the certification as Exhibits A and D, respectively, previously have been submitted to and approved by this Court,

[REDACTED]

The NSA and Central Intelligence Agency (CIA) minimization procedures attached as Exhibits B and E, respectively, as well as the FBI targeting procedures attached as Exhibit C, were submitted to this Court on April 20, 2011 [REDACTED]

[REDACTED]

[REDACTED], the NSA and CIA minimization procedures, as well as the FBI targeting procedures, are similar to, but differ in certain substantive respects from, procedures previously approved by this Court. ~~(S//OC,NF)~~

In addition, the above-captioned certification also includes amendments to the certification being reauthorized, DNI/AG 702(g) Certification [REDACTED] and its predecessors, DNI/AG 702(g) Certifications [REDACTED]. Specifically, these amendments authorize the use of the NSA and CIA minimization procedures attached as Exhibits B and E, respectively, to DNI/AG 702(g) Certification [REDACTED] in connection

~~SECRET//ORCON,NOFORN~~

with foreign intelligence information acquired in accordance with DNI/AG 702(g)

Certifications [REDACTED]¹ (S//OC,NF)

Conclusion (U)

DNI/AG 702(g) Certification [REDACTED] contains all of the elements required by the Act, and the targeting and minimization procedures included with the certification are consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. Accordingly, the Government respectfully requests, pursuant to subsection 702(k)(2) of the Act, that this Court review ex parte and in camera DNI/AG 702(g) Certification [REDACTED] and supporting documents, which are submitted herewith. The Government further requests that this Court enter an order pursuant to subsection 702(i)(3)(A) of the Act approving: DNI/AG 702(g) Certification [REDACTED] the use of the targeting and minimization procedures attached thereto as Exhibits A, B, C, D, and E in connection with acquisitions of foreign intelligence information in accordance with that certification; and the use of the minimization procedures attached as Exhibits B and E to DNI/AG 702(g) Certification [REDACTED] in

¹ The FBI minimization procedures attached to the above-captioned certification as Exhibit D are identical to the FBI minimization procedures that already have been approved for use by this Court in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED]

[REDACTED] Thus, with respect to the FBI minimization procedures currently approved for use under those certifications, no amendments are necessary. (S//OC,NF)

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

connection with foreign intelligence information acquired in accordance with DNI/AG

702(g) Certifications [REDACTED] (S//OC,NF)

Respectfully submitted,

[REDACTED]

Attorney-Advisor
National Security Division
United States Department of Justice

~~SECRET//ORCON,NOFORN~~

~~SECRET~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED]

ORDER

This matter having come before this Court pursuant to the Government's ex parte submission of the above-referenced certification in accordance with subsection 702(g)(1)(A) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and request for an order approving such certification and the use of the targeting and minimization procedures attached thereto, and full consideration having been given to the matters set forth therein, the Court finds that the above-captioned certification submitted in accordance with 50 U.S.C. § 1881a(g) contains all the required elements, and that the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States.

~~SECRET~~

Derived From:

~~Submission to the USFISC
in Docket Number captioned above~~

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such certification and the use of such procedures are approved.

Entered this ____ day of [REDACTED] 2011, at _____ Eastern Time.

Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET~~

~~SECRET//NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED]

Docket No. 702(i) 08-01

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this ____ day of [REDACTED] 2011, at _____ Eastern Time.

Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From:

~~Submission to the USFISC
in Docket Number captioned above~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] [REDACTED]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this ____ day of [REDACTED] 2011, at _____ Eastern Time.

Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From:

~~Submission to the USFISC
in Docket Number captioned above~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [REDACTED] [REDACTED]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised National Security Agency and Central Intelligence Agency minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to the Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this ____ day of [REDACTED] 2011, at _____ Eastern Time.

Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET//NOFORN~~

Derived From: Submission to the USFISC
in Docket Number captioned above

~~SECRET//ORCON,NOFORN~~

U.S. FOREIGN
INTELLIGENCE

11:03

DNI/AG 702(g) Certification

LEEANN FLYNN HALL
CLERK OF COURT

In accordance with subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and based on the representations made in the supporting affidavits of John C. Inglis, Acting Director of the National Security Agency (NSA), Robert S. Mueller, III, Director of the Federal Bureau of Investigation (FBI), and Leon E. Panetta, Director of the Central Intelligence Agency (CIA), in the above-referenced matter, the Director of National Intelligence and the Attorney General, being duly sworn, hereby certify that:¹ (S//OC,NF)

(1) there are procedures in place that have been approved² or will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court³ that are reasonably designed to --

- a. ensure that an acquisition authorized pursuant to subsection 702(a) of the Act is limited to targeting persons reasonably believed to be located outside the United States; and

[REDACTED]

(S//OC,NF)

² Specifically, the NSA targeting procedures attached herewith as Exhibit A were most recently approved by the Court on [REDACTED] 2010, in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED]. (S//OC,NF)

³ Specifically, the FBI targeting procedures attached herewith as Exhibit C are being submitted for approval by the Court. (S//OC,NF)

~~SECRET//ORCON,NOFORN~~

Classified by: The Attorney General
Reason: 1.4(c)
Declassify on: 11 April 2036

~~SECRET//ORCON,NOFORN~~

- b. prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;
- (2) the minimization procedures with respect to such acquisition --
 - a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and
 - b. have been approved⁴ or will be submitted with this certification for approval by the Foreign Intelligence Surveillance Court;⁵
- (3) guidelines have been adopted in accordance with subsection 702(f) of the Act to ensure compliance with the limitations in subsection 702(b) of the Act and to ensure that an application for a court order is filed as required by the Act;
- (4) the procedures and guidelines referred to in sub-paragraphs (1), (2), and (3) above are consistent with the requirements of the fourth amendment to the Constitution of the United States;
- (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
- (6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and
- (7) the acquisition complies with the limitations in subsection 702(b) of the Act. ~~(S)~~

On the basis of the foregoing, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, as

⁴ Specifically, the FBI minimization procedures attached herewith as Exhibit D were most recently submitted to the Court for approval in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED] 2010, and were most recently approved by the Court on [REDACTED] 2010. ~~(S//OC,NF)~~

⁵ Specifically, the NSA and CIA minimization procedures attached herewith as Exhibits B and E, respectively, are being submitted for approval by the Court. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

described above, is authorized, and such authorization shall be effective on [REDACTED], 2011, or on the date upon which the Foreign Intelligence Surveillance Court issues an order concerning this certification pursuant to subsection 702(i)(3) of the Act, whichever is later. Such targeting is authorized for a period of one year from the effective date of this authorization. This authorization reauthorizes DNI/AG 702(g) Certification [REDACTED]

[REDACTED]

which became effective on [REDACTED] 2010. ~~(S//OC,NF)~~

**Amendment 4 to DNI/AG 702(g) Certification [REDACTED]
Amendment 3 to DNI/AG 702(g) Certification [REDACTED] and
Amendment 2 to DNI/AG 702(g) Certification [REDACTED]**

Furthermore, in accordance with subsection 702(i)(1)(C) of the Act, DNI/AG 702(g) Certifications [REDACTED] are hereby amended. Specifically, the use of the NSA and CIA minimization procedures attached herewith as Exhibits B and E, respectively, in connection with foreign intelligence information acquired in accordance with DNI/AG 702(g) Certifications [REDACTED] is authorized.⁷ Such authorization, as amended, shall be effective on [REDACTED], 2011, or on the date upon which the FISC issues an order concerning these amendments pursuant to subsection 702(i)(3) of the Act, whichever is later. All other aspects of Certifications [REDACTED] as amended, remain unaltered and are incorporated herein. ~~(S//OC,NF)~~

⁶ DNI/AG 702(g) Certification [REDACTED] was first amended by the Attorney General and the Director of National Intelligence in [REDACTED] 2009. This amendment related only to modifications to the FBI's targeting procedures. Amendments to DNI/AG 702(g) Certification [REDACTED] in [REDACTED] 2010 and [REDACTED] 2010, which related only to modifications to the minimization procedures for NSA, FBI, and CIA, were incorrectly specified as Amendment 1 and Amendment 2, respectively, to DNI/AG 702(g) Certification [REDACTED]. The amendments in July and August 2010 should have been specified as Amendment 2 and Amendment 3, respectively. ~~(S//OC,NF)~~

⁷ As certified above, these minimization procedures meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act, will be submitted for approval by the FISC, and are consistent with the requirements of the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

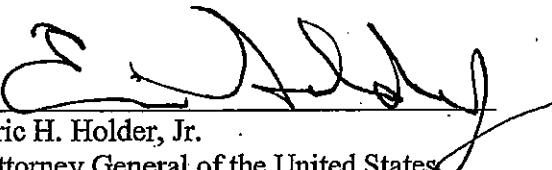
VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing certification in

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED], are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendments to DNI/AG 702(g) Certifications [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746

on April 11, 2011. (S)


Eric H. Holder, Jr.
Attorney General of the United States

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

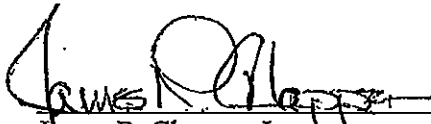
VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing certification in

[REDACTED]

[REDACTED] DNI/AG 702(g) Certification [REDACTED] are true and correct to the best of my knowledge and belief. I further declare under penalty of perjury that the facts set forth in the foregoing amendments to DNI/AG 702(g) Certifications [REDACTED] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746

on 13 April, 2011. (S)



James R. Clapper, Jr.
Director of National Intelligence

~~SECRET//ORCON,NOFORN~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE ACT

**AFFIDAVIT OF JOHN C. INGLIS, ACTING DIRECTOR,
NATIONAL SECURITY AGENCY**

2011 APR 22 AM 11:03

[REDACTED]

DNI/AG 702(g) Certification [REDACTED]

~~(S)~~ Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED] I affirm that the following is true and accurate to the best of my knowledge and belief:

1. ~~(S//NF)~~ There are reasonable procedures in place that the National Security Agency (NSA) will use to ensure that any acquisition under this certification is limited to targeting non-United States persons reasonably believed to be located outside of the United States. In addition, these targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. These targeting procedures, which are attached herewith as Exhibit A, were most recently submitted for approval to the Foreign Intelligence Surveillance Court (FISC) in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED] 2010, and were most recently approved by the FISC on [REDACTED] 2010.
2. ~~(TS//SI//NF)~~ As described below, NSA's acquisition of foreign intelligence information pursuant to this certification involves obtaining foreign intelligence information from or with the assistance of electronic communication service providers, as that term is defined in subsection 701(b)(4) of the Act.
3. ~~(TS//SI//NF)~~ NSA seeks to acquire foreign intelligence information [REDACTED]

[REDACTED]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

[REDACTED]

4. ~~(TS//SI//NF)~~ Furthermore, NSA seeks to acquire foreign intelligence information [REDACTED]

[REDACTED]

5. ~~(TS//SI//NF)~~ Pursuant to the above-referenced certification, NSA seeks to acquire foreign intelligence information concerning [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

[REDACTED]

A list [REDACTED] is attached herewith as Exhibit F. NSA believes that the non-United States persons reasonably believed to be located outside the United States who will be targeted for collection under this certification possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning [REDACTED]. Thus, a significant purpose of the acquisition is to obtain:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --
 - a. actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - b. sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
 - c. clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to --
 - a. the national defense or the security of the United States; or
 - b. the conduct of the foreign affairs of the United States.

If NSA seeks to acquire foreign intelligence information concerning [REDACTED] NSA may target under this certification non-United States persons reasonably believed to be located outside the United States who possess, are expected to receive, and/or are likely to communicate foreign intelligence information concerning [REDACTED] provided that NSA notifies the Attorney General and Director of National Intelligence within five business days of implementing such targeting. Such notification will include a description of the factual basis for NSA's determination that the [REDACTED]

6. ~~(S//NF)~~ With respect to the information NSA acquires pursuant to the above-referenced certification, NSA will follow the minimization procedures attached herewith as Exhibit B.

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

7. ~~(S//SI//NF)~~ NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to the above-referenced certification. CIA will identify to NSA the targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with the CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.
8. ~~(S//SI)~~ NSA may provide to the Federal Bureau of Investigation (FBI) unminimized communications acquired pursuant to the above-referenced certification. The FBI will identify to NSA the targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with the FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

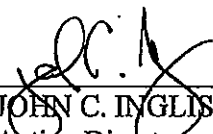
----- The remainder of this page intentionally left blank -----

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

(U) I declare under penalty of perjury that the foregoing is true and correct.

Signed this 8th day of April, 2011.



JOHN C. INGLIS
Acting Director
National Security Agency

~~TOP SECRET//COMINT//NOFORN//20320108~~

AFFIDAVIT OF ROBERT S. MUELLER, III
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE ACT
2011 APR 22 AM 11:03

DNI/AG 702(g) Certification

(S) Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED], I affirm the following is true and accurate to the best of my knowledge and belief:

1. (S) The National Security Agency (NSA) has represented to the Federal Bureau of Investigation (FBI) that, in accordance with the NSA targeting procedures attached herewith as Exhibit A, NSA may identify certain electronic communications [REDACTED] that are used by non-United States persons reasonably believed to be outside the United States and which are reasonably believed to contain foreign intelligence information [REDACTED]
2. (S) The FBI's acquisition of [REDACTED] pursuant to NSA's request is consistent with Section 702 of the Act because, *inter alia*: the acquisition will be conducted in compliance with the limitations set forth in subsection 702(b) of the Act; the acquisition will involve obtaining foreign intelligence information [REDACTED] electronic communication service providers; and a significant purpose of the acquisition is to obtain foreign intelligence information.
3. (S) In conducting the acquisition of [REDACTED] as requested by NSA, the FBI will use the procedures attached herewith as Exhibit C to determine that the requested acquisition targets non-United States persons reasonably believed to be located outside the United States.
4. (S//NF) The FBI will convey any [REDACTED] it acquires pursuant to the above-referenced certification to NSA in unminimized form without performing any further processes or procedures to ensure that the user of the [REDACTED] is a non-United States person reasonably believed to be located outside the United States. If directed by NSA, the FBI will also convey the [REDACTED] of specified [REDACTED] from the electronic communication service provider to the Central

Derived From: Multiple Sources
Declassify On: April 4, 2036

~~SECRET//NOFORN~~

Intelligence Agency (CIA) in unminimized form without performing any further processes or procedures to ensure that the user of the [REDACTED] is a non-United States person reasonably believed to be located outside the United States. NSA and CIA shall process any [REDACTED] received from the FBI in accordance with the NSA and CIA minimization procedures, respectively, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

5. ~~(S)~~ The minimization procedures that the FBI will use with respect to any [REDACTED] it acquires pursuant to the above-referenced certification are attached herewith as Exhibit D. These minimization procedures were most recently submitted for approval to the Foreign Intelligence Surveillance Court (FISC) in connection with Amendment 1 to DNI/AG 702(g) Certification [REDACTED] on [REDACTED], 2010, and were most recently approved by the FISC on [REDACTED] 2010.
6. ~~(S)~~ NSA may acquire, pursuant to the above-referenced certification, unminimized communications as those communications are transmitted. Such unminimized communications may contain foreign intelligence information relating to the lawful functions and responsibilities of the FBI's counterterrorism, counterintelligence, and national security activities. Accordingly, the FBI may request and receive such unminimized communications from NSA. The FBI will identify to NSA the targeted selectors for which the FBI seeks the dissemination of unminimized communications. The minimization procedures that the FBI will use with respect to any unminimized communications it receives from NSA are attached herewith as Exhibit D.


---- The remainder of this page intentionally left blank ----

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

I declare under penalty of perjury that the foregoing is true and correct.

Signed this 8th day of April 2011.



ROBERT S. MUELLER, III
Director, Federal Bureau of Investigation

~~SECRET//NOFORN~~

~~TOP SECRET//NOFORN~~

U.S. FEDERAL
INTELLIGENCE
SURVEILLANCE ACT

AFFIDAVIT OF THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

2011 APR 22 AM 11:01

[REDACTED]

DNI/AG 702(g) Certification [REDACTED]

CLERK OF COURT

~~(TS//NF)~~ Pursuant to subsection 702(g)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), and in support of DNI/AG 702(g) Certification [REDACTED] I affirm the following is true and accurate to the best of my knowledge and belief:

1. ~~(S)~~ As Director of the Central Intelligence Agency (CIA), I am responsible for the collection of foreign intelligence through human sources and by other appropriate means. These functions are carried out by and through CIA. The mission of CIA includes the collection, production, and dissemination of foreign intelligence and counterintelligence, including information not otherwise obtainable. This includes the conduct of clandestine espionage or counterintelligence activities abroad.

2. ~~(TS//NF)~~ Pursuant to the above-referenced certification, the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) may acquire unminimized communications. [REDACTED]

3. ~~(TS//NF)~~ [REDACTED]

4. ~~(TS//NF)~~ [REDACTED]

~~TOP SECRET//NOFORN~~

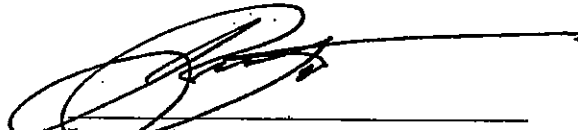
~~TOP SECRET//NOFORN~~



5. ~~(TS//NF)~~ I have reviewed the minimization procedures attached herewith as Exhibit E. CIA will follow these minimization procedures with respect to communications acquired pursuant to the above-referenced certification.

I declare under penalty of perjury that the foregoing is true and correct.

Signed this 6th day of April 2011.



Leon E. Panetta
Director, Central Intelligence Agency

~~TOP SECRET//NOFORN~~

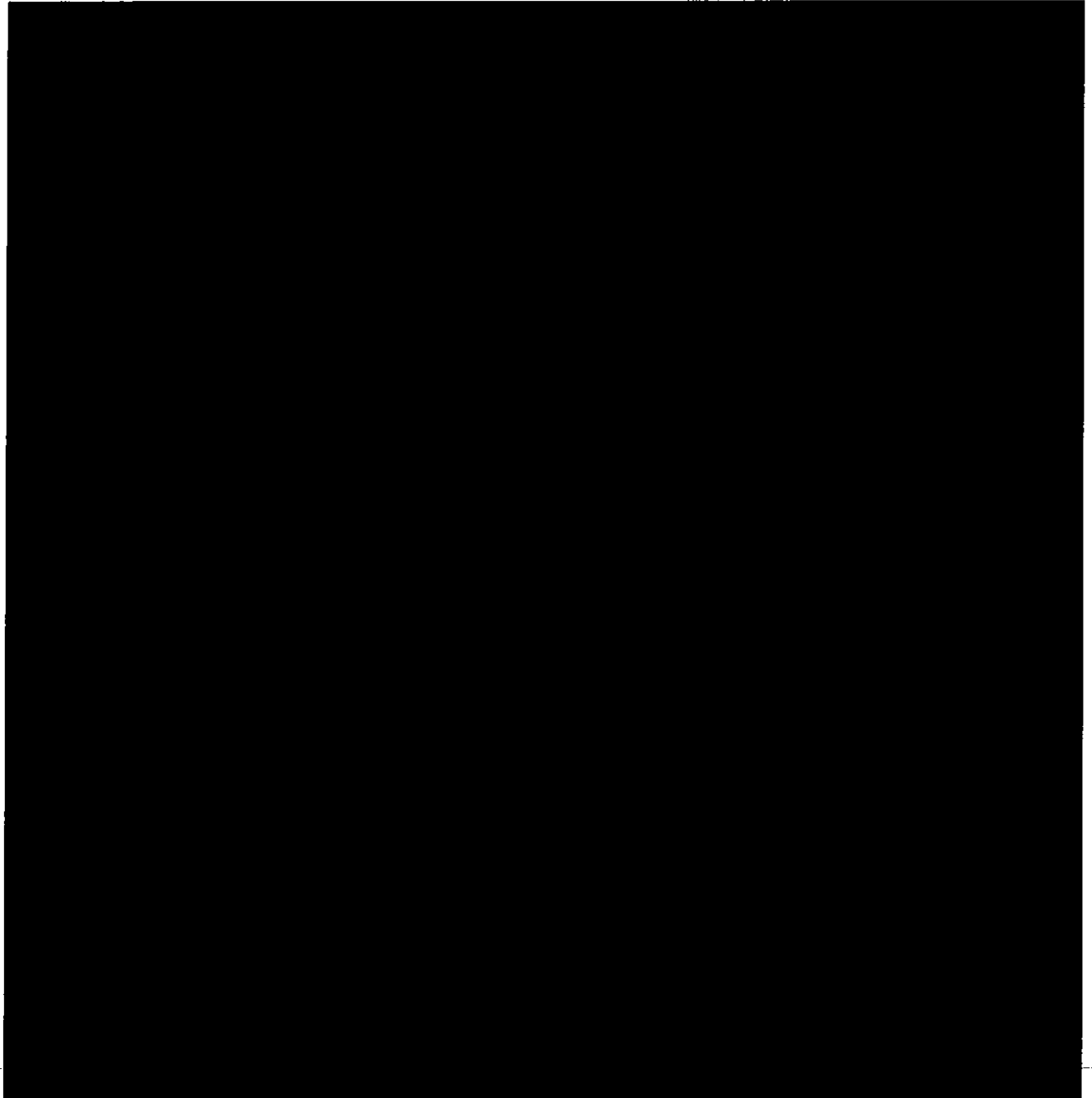
~~TOP SECRET//COMINT//NOFORN//20320108~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING
NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED
OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT OF 1978, AS AMENDED

2009 JUL 28 PM 3:14
CLERK OF COURT



Derived From: NSA/CSSM 1-52

Dated: 20070108

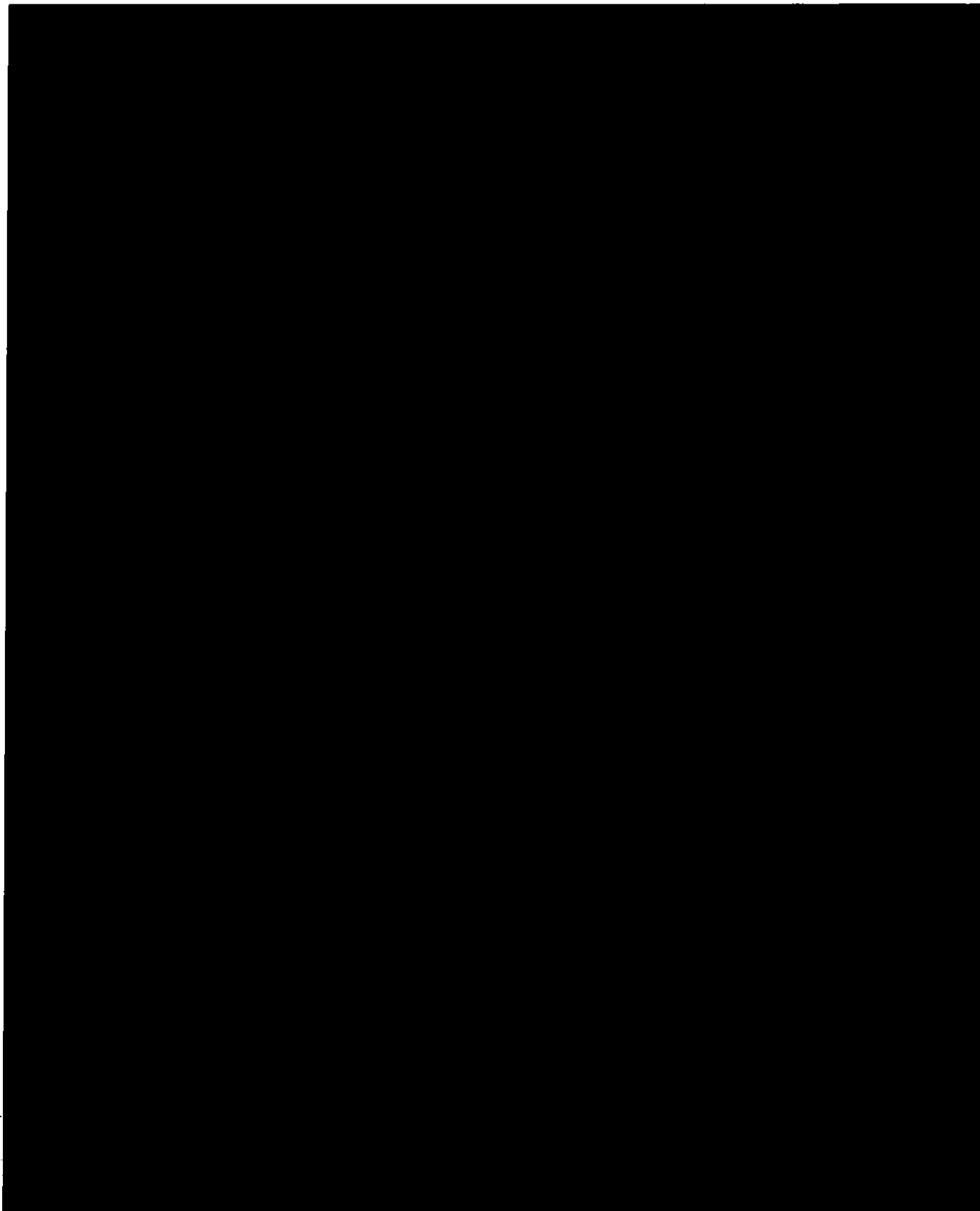
Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

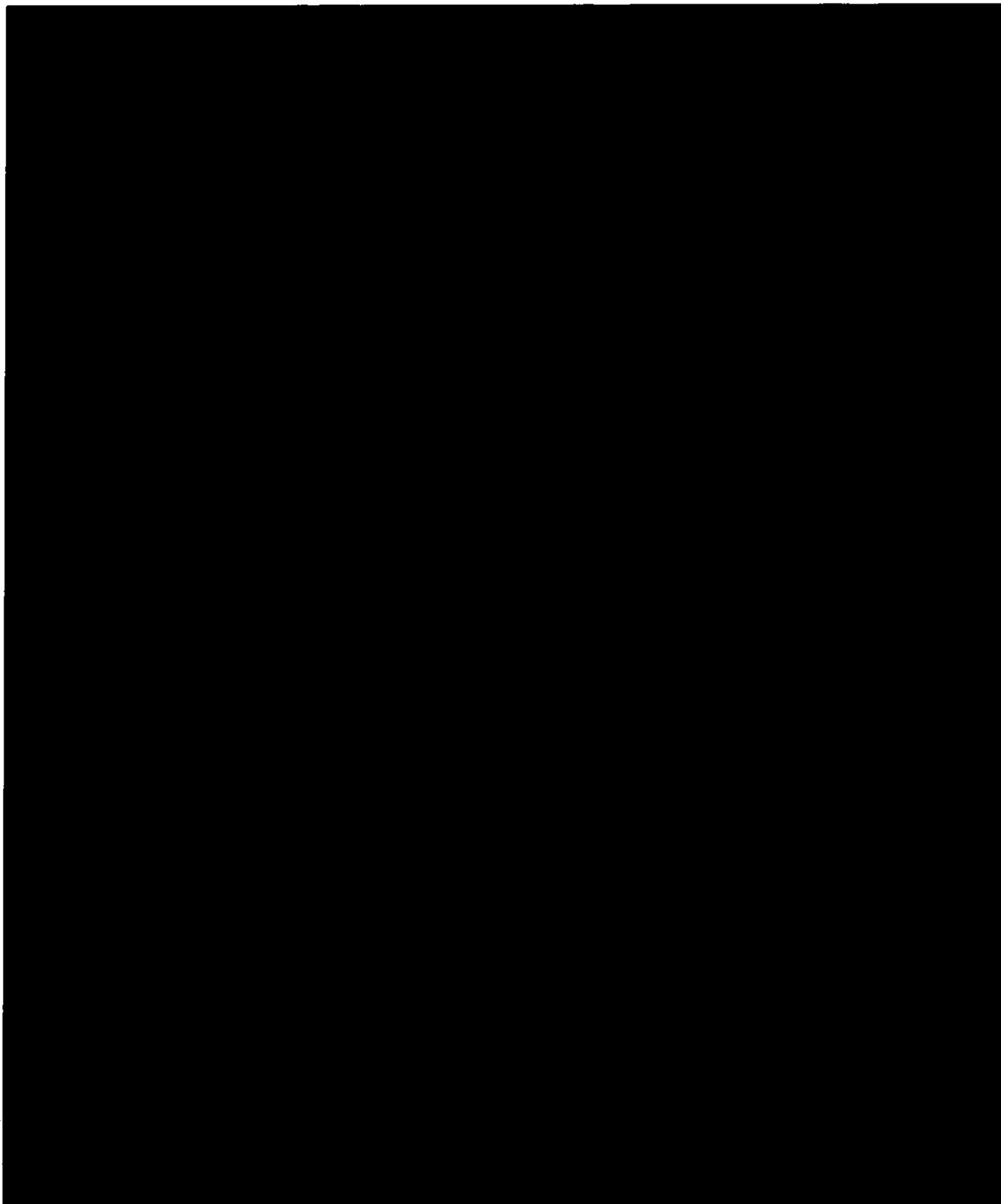


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

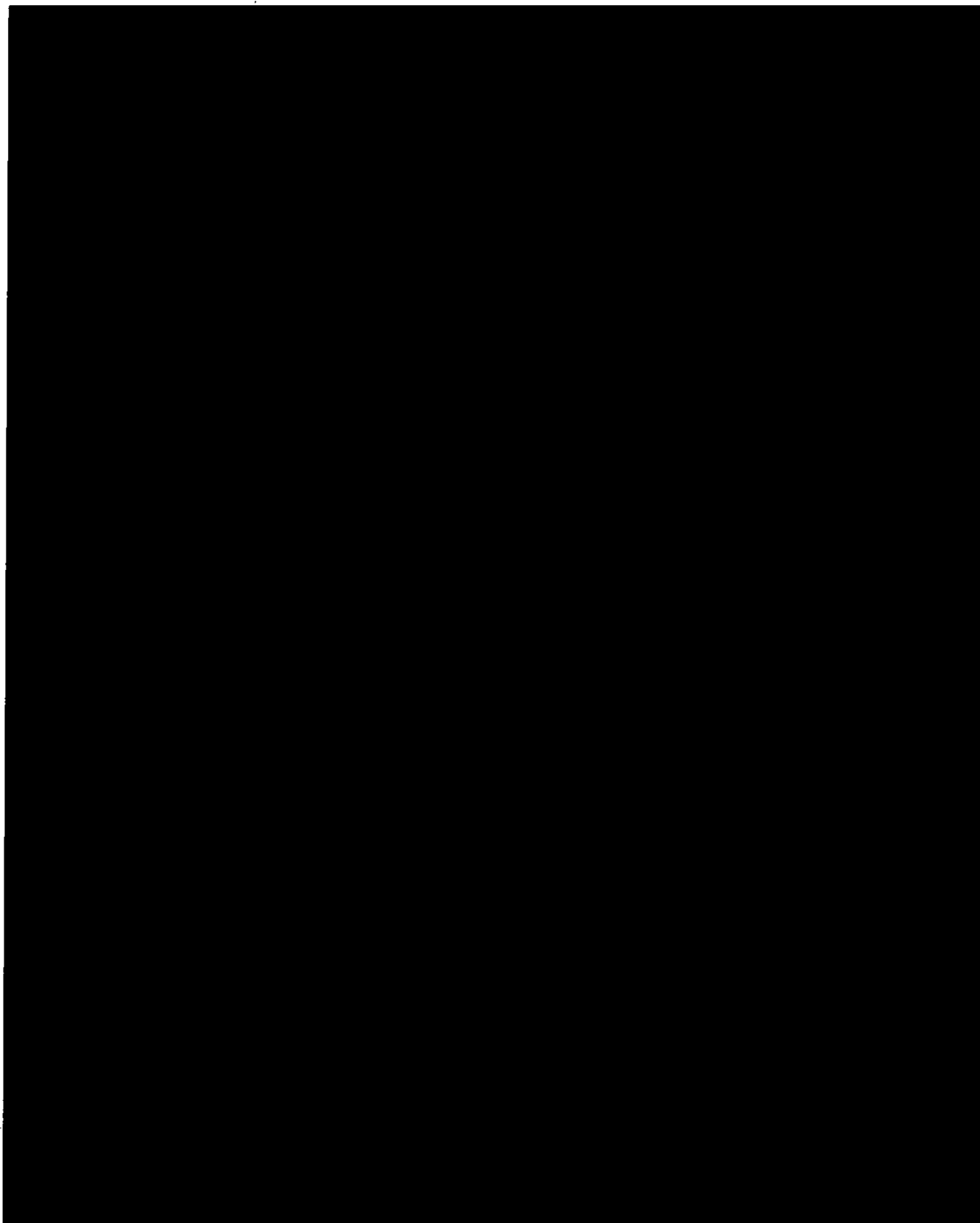


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

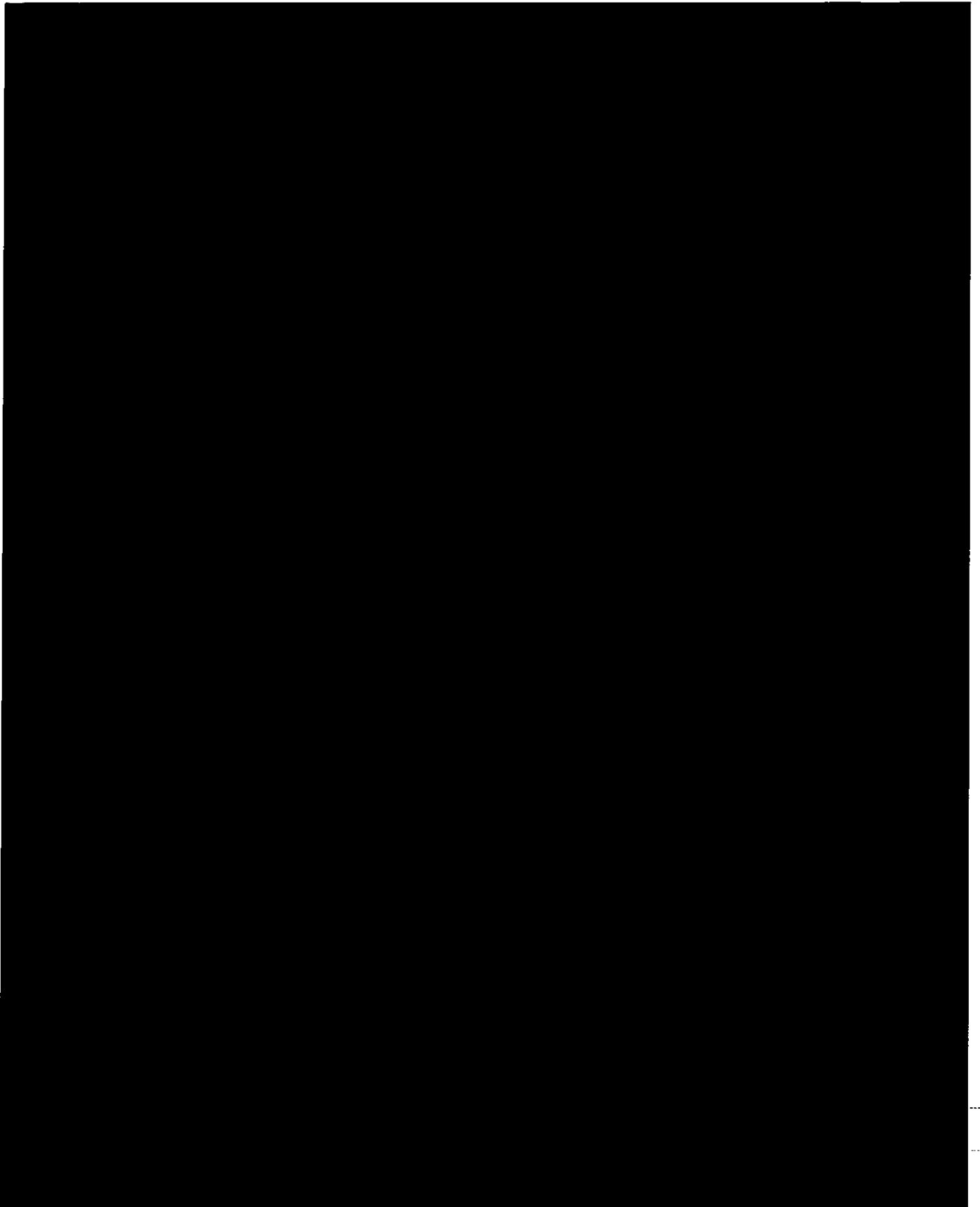


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

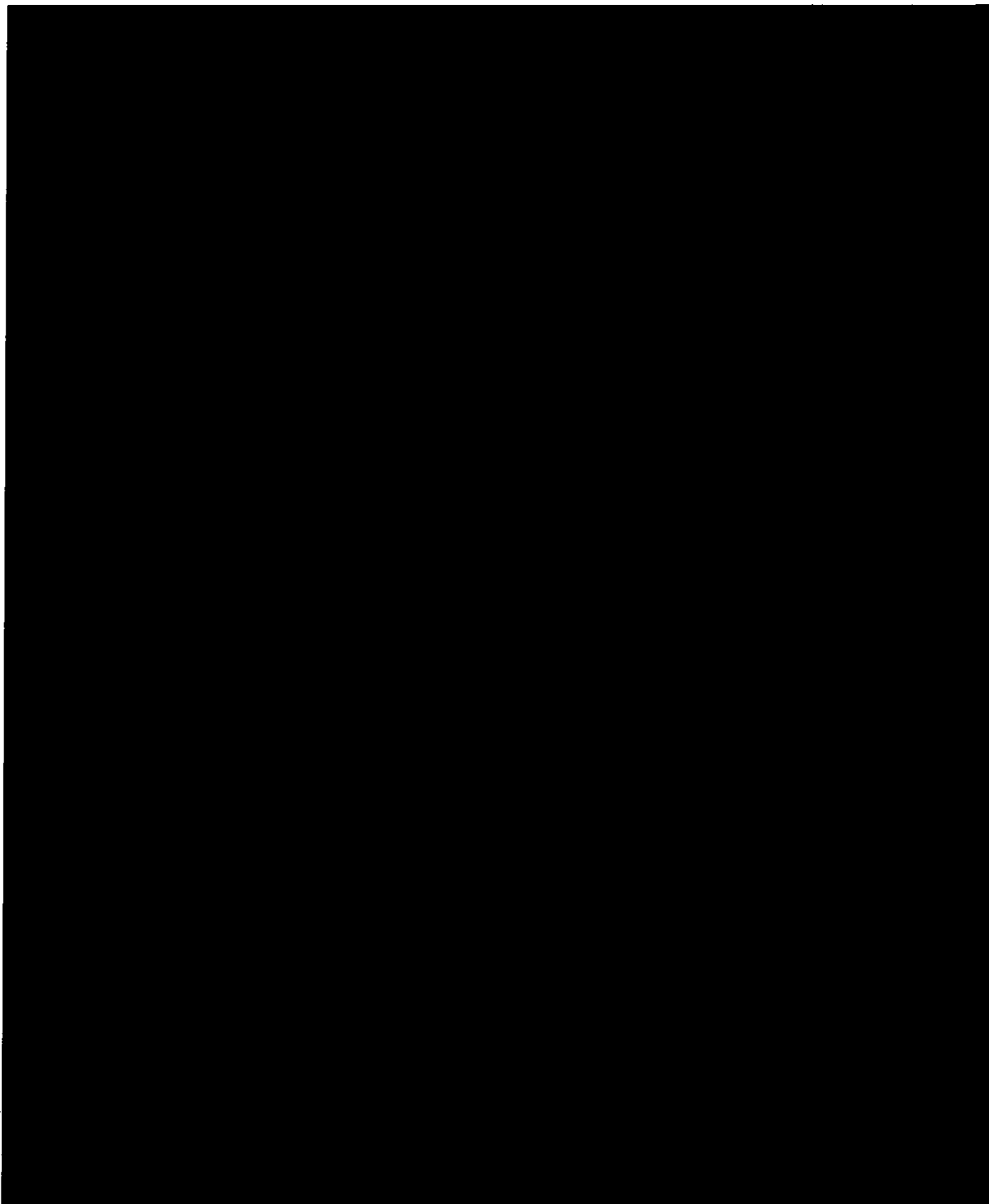


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

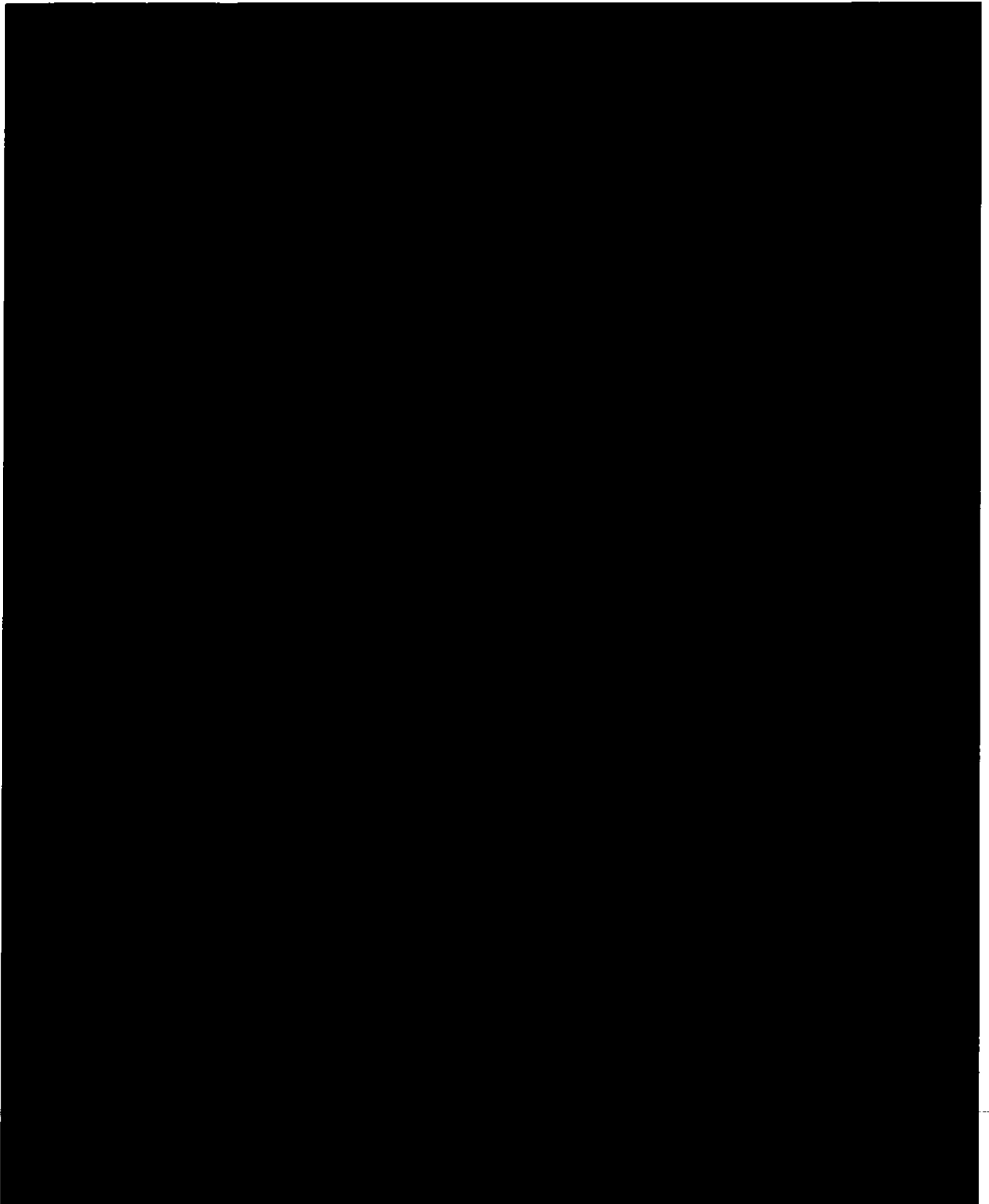


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~

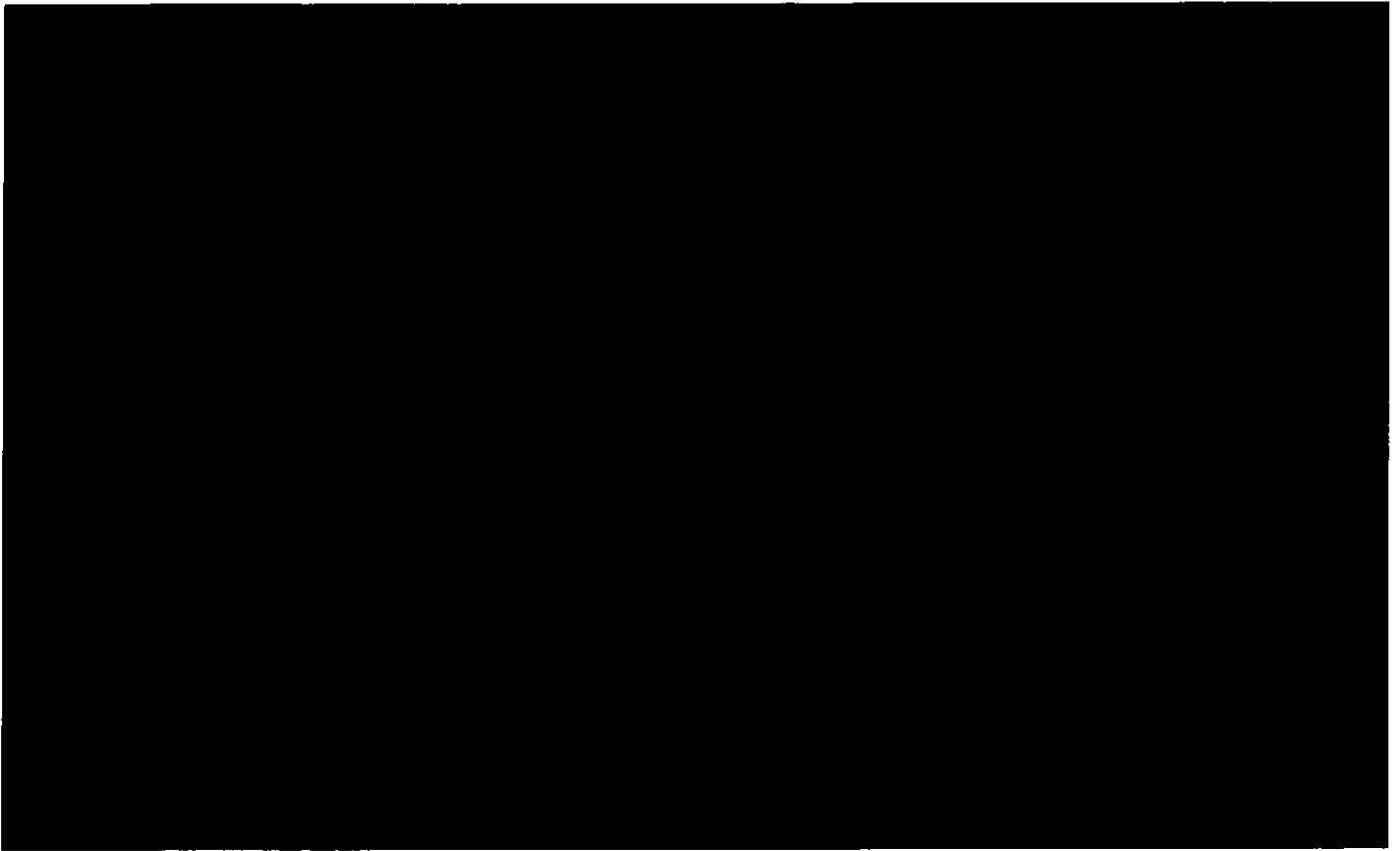


~~TOP SECRET//COMINT//NOFORN//20320108~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN//20320108~~



~~TOP SECRET//COMINT//NOFORN//20320108~~

EXHIBIT B**MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN
CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE
INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT OF 1978, AS AMENDED**
JULY 1978
APR 20 11:20
CLERK OF COURT**Section 1 - Applicability and Scope (U)**

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). (U)

Section 2 - Definitions (U)

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

- (a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party. (U)
- (b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. (U)
- (c) Communications of a United States person include all communications to which a United States person is a party. (U)

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

~~SECRET//COMINT//NOFORN//20320108~~

- (d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)
- (e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. ~~(S//SI)~~
- (f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//SI)~~
- (g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)
- (h) Publicly-available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)
- (i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~
- (j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)
- (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)
 - (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

~~SECRET//COMINT//NOFORN//20310108~~

- (3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with 8 U.S.C. § 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)
- (4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

Section 3 - Acquisition and Processing - General (U)

(a) Acquisition (U)

The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. (S//SI)

(b) Monitoring, Recording, and Processing (U)

- (1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. ~~(S//SI)~~
- (2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, 6, and 8 of these procedures. ~~(C)~~
- (3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

~~SECRET//COMINT//NOFORN//20320108~~

- (4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5, 6, and 8 of these procedures.

~~(S//SI)~~

- (5) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph. ~~(S//SI)~~

- (6) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below. ~~(S//SI)~~

(c) Destruction of Raw Data ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as facsimile, telex, computer data, or equipment emanations, will be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet such retention standards and that are known to contain communications of or concerning United States persons will be destroyed upon recognition, and may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. The communications that may be retained include electronic communications acquired because of limitations on NSA's ability to filter communications. ~~(S//SI)~~

(d) Change in Target's Location or Status ~~(S//SI)~~

- (1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay. ~~(S//SI)~~
- (2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact

~~SECRET//COMINT//NOFORN//20320108~~

~~SECRET//COMINT//NOFORN//20310108~~

located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. ~~(S//SI)~~

Section 4 - Acquisition and Processing - Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. ~~(S//SI)~~

Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: ~~(S)~~

- (1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the Federal Bureau of Investigation (FBI) (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; ~~(S)~~
- (2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; ~~(S)~~
- (3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the

~~SECRET//COMINT//NOFORN//20320108~~

~~SECRET//COMINT//NOFORN//20310108~~

FBI and/or disseminated to other elements of the United States Government. Such communications may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//SI)~~

- a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//SI)~~
- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or ~~(S//SI)~~

- (4) the communication contains information pertaining to a threat of serious harm to life or property. ~~(S)~~

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. ~~(S//SI)~~

Section 6 - Foreign Communications of or Concerning United States Persons (U)

(a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

- (1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.
 - a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

~~SECRET//COMINT//NOFORN//20320108~~

- b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signals Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;
- (2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or
- (3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S//SI)~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

- (1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;
- (2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;
- (3) the communication or information indicates that the United States person may be:
 - a. an agent of a foreign power;
 - b. a foreign power as defined in Section 101(a) of the Act;
 - c. residing outside the United States and holding an official position in the government or military forces of a foreign power;
 - d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
 - e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

~~SECRET//COMINT//NOFORN//20310108~~

- (4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;
 - (5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications security vulnerability, but only after the agency that originated the information certifies that it is properly classified;
 - (6) the communication or information indicates that the United States person may be engaging in international terrorist activities;
 - (7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or
 - (8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)
- (c) Provision of Unminimized Communications to CIA and FBI ~~(S//NF)~~
- (1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI//NF)~~
 - (2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI)~~

Section 7 - Other Foreign Communications (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

(U)

~~SECRET//COMINT//NOFORN//20320108~~

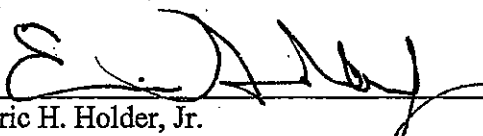
~~SECRET//COMINT//NOFORN//20310108~~Section 8 - Collaboration with Foreign Governments ~~(S//SI)~~

- (a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. ~~(S)~~
- (b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: ~~(S)~~
- (1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. ~~(S)~~
 - (2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. ~~(S)~~
 - (3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. ~~(S)~~
 - (4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. ~~(S)~~

~~SECRET//COMINT//NOFORN//20320108~~

- (5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. ~~(S)~~

4-11-11
Date


Eric H. Holder, Jr.
Attorney General of the United States

~~SECRET//NOFORN//21 JULY 2034~~

EXHIBIT C

2011 APR 20 AM 11:20
U.S. FEDERAL
INTELLIGENCE
SURVEILLANCE
COURT

PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION FOR
TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE
LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN
INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

~~(S)~~ These procedures address: (I) the process the Federal Bureau of Investigation (FBI) will use in acquiring foreign intelligence information, [REDACTED] by targeting electronic communications accounts/addresses/identifiers designated by the National Security Agency (NSA) [REDACTED] as being used by non-United States persons reasonably believed to be located outside the United States, (II) the FBI's documentation of that process, and (III) compliance and oversight.

I. (U) DETERMINATION OF WHETHER A PERSON IS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES AND NOT A UNITED STATES PERSON

1. ~~(S)~~ [REDACTED] NSA will follow its targeting procedures, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(d) of the Act, for determining that the user of the [REDACTED] is a person reasonably believed to be located outside the United States and is not a United States person. NSA will also be responsible for determining that a significant purpose of the acquisition is to obtain foreign intelligence information.
2. ~~(S)~~ NSA will provide the FBI with identifying information of any [REDACTED] together with an explanation of NSA's conclusion that the user of the [REDACTED] is a person reasonably believed to be located outside the United States and its determination regarding the non-United States person status of the user. NSA will also represent that a significant purpose of [REDACTED] is to obtain foreign intelligence information and that the purpose of such acquisition is not to intentionally target a particular, known person reasonably believed to be in the United States.
3. ~~(S)~~ The FBI, in consultation with NSA, will review and evaluate the sufficiency of: (a) NSA's explanation for its reasonable belief that the user of the [REDACTED] is located outside of the United States; and (b) information provided by NSA concerning the [REDACTED] user's non-United States person status.

Classified By: PSCG
Reason: E.O. 12958 Section 1.4((c))
Declassify On: 21 July 2034
~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

4. ~~(S)~~ In the ordinary course of determining whether to

[REDACTED]

- a. ~~(S)~~

[REDACTED]

- b. ~~(S)~~

[REDACTED]

5. ~~(S)~~ Unless the FBI [REDACTED] the user of the [REDACTED]
[REDACTED] is a United States person or is located inside of the United States, the FBI will

[REDACTED]

6. ~~(S//NF)~~

[REDACTED]

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

[REDACTED]

All such communications retained by the FBI will be processed in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act.

7. ~~(S)~~ If NSA analysis of [REDACTED] indicates that a user of a [REDACTED] from which [REDACTED] pursuant to these procedures is actually located within the United States or is a United States person, NSA will promptly [REDACTED]
8. ~~(S)~~ If the FBI [REDACTED] is not appropriate for tasking under section 702 (i.e., because the user of the [REDACTED] is a United States person and/or is located inside of the United States), the FBI will inform NSA, and the FBI will not [REDACTED] of the [REDACTED] until the FBI determines that the [REDACTED] is in fact appropriate for tasking under section 702.
9. ~~(S)~~ In addition, the FBI will take appropriate action, which may include the [REDACTED]

[REDACTED]

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN//21 JULY 2034~~

II. (U) DOCUMENTATION

10. ~~(S)~~ The FBI will ensure the retention of information it receives from NSA concerning the non-United States person status of the user of the [REDACTED] and the factual basis for NSA's determination that the user of the [REDACTED] is reasonably believed to be located outside the United States in accordance with the National Archives and Records Administration (NARA) and, as appropriate, the FBI's Records Management Division and/or Security Division standards, policies, and guidelines.

11. ~~(S)~~ [REDACTED]

III. (U) COMPLIANCE AND OVERSIGHT

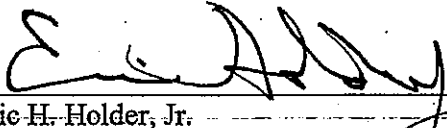
12. ~~(S)~~ The FBI will develop and deliver training regarding the applicable procedures to ensure that all personnel responsible for [REDACTED] under these procedures understand their responsibilities with respect to [REDACTED]. The FBI has established processes for determining which [REDACTED] and for ensuring that [REDACTED] and the related [REDACTED] are accessible only to those who are authorized and have had the proper training.

13. ~~(S)~~ The FBI Inspection Division will conduct oversight of the FBI's exercise of these procedures. This oversight will include periodic reviews by FBI Inspection Division personnel to evaluate the implementation of the procedures and the training given to relevant personnel. Such reviews will occur at least once every quarter.

14. ~~(S)~~ The DOJ and ODNI will conduct oversight of the FBI's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of these procedures. Such reviews will occur at least once every sixty days.

15. ~~(S)~~ The FBI will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by FBI personnel within five business days of learning of the incident.

4-11-11
Date


Eric H. Holder, Jr.

Attorney General of the United States

~~SECRET//NOFORN//21 JULY 2034~~

~~SECRET//NOFORN~~U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT




EXHIBIT D

2009 JUL 29 PM 3:14
CLERK OF COURT

**MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF
INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN
INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN
INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED**

These Federal Bureau of Investigation (FBI) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

With respect to any unminimized communications acquired pursuant to section 702 of the Act, the FBI will apply its standard minimization procedures as described in the Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act (adopted October 21, 2008) ("Standard Minimization Procedures"), with the following modifications: ~~(S)~~

- a. References to "information acquired pursuant to FISA" and "FISA-acquired information" will be understood to also include communications acquired pursuant to section 702 of the Act. (U)
- b.  ~~(S)~~
- c. References to "target" will be understood to refer to the user(s) of a targeted selector, account, or  ~~(S)~~
- d. Section II.A ("Acquisition – Electronic Surveillance") will not apply. (U)
- e. Subparagraphs 1 through 5 of Section II.B ("Acquisition – Physical Search, including of Electronic Data") will be replaced in their entireties by the following subparagraphs: ~~(S)~~
 1. The FBI may acquire  pursuant to section 702 of the Act only in accordance with FBI targeting procedures that have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to section 702(d) of the Act. ~~(S)~~
 2. Any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time

Derived From: Multiple Sources
Declassify On: July 21, 2034

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

such communication is acquired or is subsequently determined to be a United States person will be removed from FBI systems upon recognition, unless the Director or Deputy Director of the FBI specifically determines in writing that such communication is reasonably believed to contain significant foreign intelligence information, evidence of a crime that has been, is being, or is about to be committed, or information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. Notwithstanding the above, if any such communications indicate that a person targeted under section 702 has entered the United States, nothing in these procedures shall prevent the FBI from retaining and providing to the National Security Agency (NSA) and Central Intelligence Agency (CIA) technical information derived from such communication for collection avoidance purposes. ~~(S)~~

3. As soon as FBI personnel recognize that an acquisition of a communication under section 702 of this Act is inconsistent with any of the limitations set forth in section 702(b),¹ the FBI will purge the communication and destroy all other copies of that communication that are accessible to any end user electronically or in hard copy. Any electronic copies of the communication that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted communication will not be accessible to any user and will be deleted from any stored system. ~~(S)~~

- f. Paragraph 4 of Section III.B will be replaced in its entirety with the following:

Required training on the Standard Minimization Procedures and the FBI's policies regarding access to raw FISA-acquired information before granting access to raw FISA-acquired information. ~~(S)~~

¹ Subsection 702(b) provides that "[a]n authorization authorized under subsection (a) --

- (1) may not intentionally target any person known at the time of the acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be located in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." (U)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- g. The following will be added as Paragraph 6 to Section III.B:

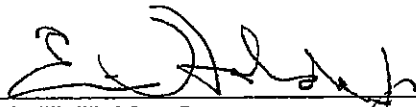
With respect to information acquired pursuant to section 702 of the Act, only those FBI personnel who have received training on the application of these "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" may be designated as case coordinators. All FBI personnel having access to information acquired pursuant to section 702 of the Act will be informed of and provided access to these minimization procedures. ~~(S)~~

- h. Section III.C.3 ("Categories of Non-Pertinent and Sensitive Information") will not apply. ~~(S)~~
- i. In Section III.E ("Retention of Attorney-Client Communications"), the second sentence of the preamble (i.e., "In certain cases, however, the Government may propose and/or the FISC may order the use of supplemental procedures.") shall not apply. Furthermore, all remaining references to the FISC in this section shall be replaced by DOJ-NSD. ~~(S)~~
- j. The time limits described in Section III.G ("Time Limits for Retention") as applied to communications acquired pursuant to section 702 of the Act will be measured from the expiration date of the certification authorizing the collection. ~~(S)~~
- k. Section IV.E ("Dissemination Under [REDACTED]") will be replaced in its entirety with the following paragraph: ~~(S)~~

With respect to any communications that the FBI acquires from an electronic communication service provider pursuant to Section 702 of the Act, the FBI may convey such communications to the NSA and CIA in unminimized form. The NSA and CIA shall process any [REDACTED] received from the FBI pursuant to these procedures in accordance with the NSA and CIA minimization procedures, respectively, adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S)~~

- l. Section V.C ("Minimization Briefings") will not apply. ~~(S)~~

7-28-09
Date


Eric H. Holder, Jr.
Attorney General of the United States

~~SECRET//NOFORN~~

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET~~

**STANDARD MINIMIZATION PROCEDURES FOR FBI ELECTRONIC
SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED
UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)**

EFFECTIVE: November 1, 2008

~~Classified by: Michael Mukasey, Attorney General
Reason: 1.4(c)
Declassify on: October 21, 2033~~

~~SECRET~~

~~SECRET~~TABLE OF CONTENTS

I. GENERAL PROVISIONS (U).....	1
II. ACQUISITION (U).....	4
A. Acquisition – Electronic Surveillance (U)	4
B. Acquisition – Physical Search, [REDACTED] (S).....	5
1. Personnel Authorized to Conduct Physical Search (U)	5
2. Conducting Physical Search (U)	5
a. Areas of search (U)	6
b. Manner of search (U)	6
i. [REDACTED] (S).....	6
ii. Temporary Removal (S)	7
iii. Destructive Testing (U).....	7
c. United States Person [REDACTED] (S).....	7
3. Physical Search Involving Mail or Private Couriers (U)	7
4. Record of Information Collected in Physical Search (U).....	8
5. Report of Physical Search (U).....	8
C. Acquisition – Third Parties (U)	8
III. RETENTION (U)	9
A. Retention – Storage of FISA-acquired Information (U).....	9
B. Retention – Access to FISA-acquired Information (U).....	10
C. Retention – Review and Use of FISA-acquired Information (U).....	12
1. General Provisions (U).....	12
2. Third-Party Information (U).....	13
3. Categories of Non-Pertinent and Sensitive Information (U).....	14

~~SECRET~~

~~SECRET~~

D. Retention [REDACTED] (S).....	16
E. Retention of Attorney-Client Communications (U).....	17
1. Target charged with a crime pursuant to the United States Code (U).....	17
2. Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States (U).....	19
3. Privileged communications involving targets and other persons not charged with a crime in the United States (U).....	21
F. Additional Procedures for Retention, Use and Disclosure of FISA Information (U).....	22
G. Time Limits for Retention (U).....	25
1. [REDACTED]	
2. [REDACTED]	
3. [REDACTED]	
4. [REDACTED]	

IV. DISSEMINATION (U)..... 27

A. Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies (U).....	27
1. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1) (U).....	27
2. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2) (U).....	28
B. Dissemination of Evidence of a Crime to Federal, State, Local and Tribal Officials (U).....	28

~~SECRET~~

~~SECRET~~

C. Dissemination of Foreign Intelligence Information Concerning United States Persons to Foreign Governments (U).....	29
D. [REDACTED].....	30
E. [REDACTED].....	32
F. [REDACTED].....	32
G. [REDACTED].....	33
V. COMPLIANCE (U).....	33
A. Oversight (U).....	33
B. Training (U).....	35
C. Minimization Briefings (U).....	35
VI. Interpretation (U).....	35
VII. Review of Procedures (U)	36

~~SECRET~~

~~SECRET~~

I. GENERAL PROVISIONS (U)

A. In accordance with 50 U.S.C. §§ 1801(h) and 1821(4), these procedures govern the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons that the Federal Bureau of Investigation (FBI) obtains pursuant to orders issued by the Foreign Intelligence Surveillance Court (FISC) or emergency authorizations by the Attorney General under the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), 50 U.S.C. §§ 1801-1811 and 1821-1829. For the purpose of these procedures, the term "applicable FISA authority" refers to both FISC-ordered and Attorney General authorized electronic surveillance or physical search conducted in a particular case pursuant to FISA. The Attorney General has adopted these procedures after concluding that they meet the requirements of 50 U.S.C. §§ 1801(h) and 1821(4) because they are specific procedures that are reasonably designed in light of the purpose and technique of the particular surveillance or physical search to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information and otherwise comport with the statutory definition of minimization procedures. In accordance with 50 U.S.C. § 403-1(f)(6), the Director of National Intelligence (DNI) has provided assistance to the Attorney General with respect to the dissemination procedures set forth herein so that FISA-acquired information may be used efficiently and effectively for foreign intelligence purposes. (U)

~~SECRET~~

~~SECRET~~

B. Pursuant to 50 U.S.C. §§ 1806(a) and 1825(a), no information acquired pursuant to FISA may be used or disclosed by Federal officers or employees except for lawful purposes.

Information acquired from electronic surveillance or physical search conducted under FISA concerning United States persons may be used and disclosed by Federal officers and employees without the consent of the United States persons only in accordance with these minimization procedures and any modified or supplemental minimization procedures that may apply. These procedures do not apply to publicly available information concerning United States persons, nor do they apply to information that is acquired, retained, or disseminated with a United States person's consent. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S)

C. These procedures adopt the definitions set forth in 50 U.S.C. § 1801, including those for the terms "foreign intelligence information" and "United States person." [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S)

D. If FBI personnel, which, for the purposes of these procedures, includes all contractors and others authorized to work under the direction and control of the FBI on FISA related matters, encounter a situation that they believe requires them to act inconsistently with these procedures in order to protect the national security of the United States, enforce the criminal law, or protect life or property from serious harm, those personnel immediately should contact FBI

Headquarters and the Office of Intelligence of the National Security Division of the Department of Justice (NSD) to request that these procedures be modified. The United States may obtain modifications to these procedures with the approval of the Attorney General and a determination by the FISC that the modified procedures meet the definition of minimization procedures under sections 1801(h) and/or 1821(4) of FISA. (U)

E. If, in order to protect against an immediate threat to human life, the FBI determines that it must take action in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the FISC, the FBI shall report that activity promptly to the NSD, which shall notify the FISC promptly of such activity. (U)

F. Nothing in these procedures shall restrict the FBI's performance of lawful oversight functions of its personnel. (U)

~~SECRET~~

~~SECRET~~

II. ACQUISITION (U)

A. Acquisition – Electronic Surveillance. (U)

1. Prior to initiating electronic surveillance, the FBI shall verify that the facility or place at which it will direct surveillance is the facility or place specified in the applicable FISA authority. The FBI is under a continuing obligation to verify that the authorized target of the surveillance uses or is about to use the facility or place at which the surveillance is directed during the authorized period of surveillance. The FBI shall terminate electronic surveillance of a facility or place as soon as it determines that the authorized target of the electronic surveillance no longer uses, nor is about to use, the facility or place, and shall promptly notify the NSD of such termination. (U)

2. When conducting electronic surveillance of a facility or place pursuant to the applicable FISA authority, the FBI may acquire, using the means and to the extent approved by the court or authorized by the Attorney General for that facility or place: (a) all information or communications transmitted to or from the facility or place; (b) all communications that occur at such facility or place; (c) all visual, aural, and other non-verbal information that the approved surveillance device(s) can acquire at such facility or place; and (d) all information, communications, or other data processed at such facility or place by computers or other equipment present at the facility or place. To the extent consistent with the electronic surveillance approved by the Court or authorized by the Attorney General, the FBI may, at its discretion, automatically record all information, communications and data that it acquires, and also may conduct live monitoring of such acquisition. ~~(S)~~

~~SECRET~~

~~SECRET~~

3. Notwithstanding Section II.A.2, the FBI shall, to the extent reasonably feasible:

(a) use means of surveillance that are designed to limit the acquisition of nonpublicly available information or communications of or concerning unconsenting United States persons that are not foreign intelligence information relating to a target of the surveillance; and (b) place surveillance devices in locations within a facility or place at which surveillance is directed only where they are likely to acquire foreign intelligence information relating to a target of the surveillance. ~~(S)~~

B. Acquisition – Physical Search, [REDACTED] ~~(S)~~

1. Personnel Authorized to Conduct Physical Search. (U)

Physical search shall be conducted only by: (i) appropriately authorized and trained personnel of the FBI, not including contractors; (ii) [REDACTED]

[REDACTED] (iii) [REDACTED]

[REDACTED] Pursuant to 50 U.S.C. § 1824(e)(2)(B)-(D), other persons, [REDACTED], may assist in the physical search as specified in the applicable FISA authority. ~~(S)~~

2. Conducting Physical Search. (U)

Prior to initiating physical search, the FBI shall verify that the premises or property at which it will conduct physical search is the premises or property specified in the applicable FISA authority. The FBI shall conduct physical search with the minimum intrusion necessary to acquire the foreign intelligence information sought. Personnel conducting physical search shall exercise reasonable judgment in determining whether the information, material, or property

~~SECRET~~

~~SECRET~~

revealed through the search reasonably appears to be foreign intelligence information relating to a target of the search or evidence of a crime. The FBI shall conduct the search in accordance with the applicable FISA authority. (U)

a. Areas of search. For physical search of premises or property, after conducting any necessary protective sweep, the FBI shall, where reasonably feasible, limit search areas to locations within premises or property where the FBI reasonably expects that: (i) foreign intelligence information may be stored or concealed by the target; or (ii) foreign intelligence information related to the target or the activities of the target may be found. (U)

b. Manner of Search. The FBI may conduct physical search using the methods most suitable for acquiring the foreign intelligence information sought in light of the particular circumstances of the search. When conducting a physical search of electronic data, the FBI may acquire all information, communications, or data relating to the target in accordance with the applicable FISA authority. Methods used to conduct physical search may include: inspection; examination; reproduction; temporary removal; marking for identification; testing; alteration; substitution; or seizure of information, material, or property. (U)

i.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

~~SECRET~~

~~SECRET~~

- ii. Temporary Removal. The FBI may temporarily remove information, material, or property for technical, scientific, or other reasonably necessary examination, and for any other purpose approved by the Court. ~~(S)~~
- iii. Destructive Testing. The FBI may conduct destructive testing of material discovered in a physical search only when such testing is provided for in the applicable FISA authority or in case of emergency when reasonably necessary to protect against immediate threat to public safety. (U)

c. United States Person Information, Material, or Property. The FBI may intentionally alter, substitute, or seize information, material, or property belonging to a United States person only when reasonably necessary to prevent serious injury, loss of life, crime, damage to property, or damage to the national security of the United States. The preceding sentence does not preclude the alteration or substitution of material or property that is necessary to effect a physical search of electronic data in accordance with the applicable FISA authority.

~~(S)~~

3. Physical Search Involving Mail or Private Couriers. (U)

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

~~SECRET~~

~~SECRET~~

b. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] ~~(S)~~

4. Record of Information Collected in Physical Search. (U)

The FBI shall keep records identifying all information, material, or property acquired during a physical search. (U)

5. Report of Physical Search. (U)

Within seven business days following the execution of a physical search, or receiving notice that a search has been executed, and for which the FISC ordered that a search return be filed, the FBI shall notify the NSD of the date the search took place. The preceding requirement shall not apply to physical searches of electronic data. ~~(S)~~

C. Acquisition – Third Parties. (U)

“Third-party information” is: (a) nonpublicly available information of or concerning an unconsenting United States person who is not the authorized target of the particular FISA collection, or (b) the material or property of a United States person who is not the authorized target of the particular FISA collection. Third-party information may include the communications or property of family members, coworkers or others, who are not the targets of the collection, but who share facilities, premises or property with the target. Third-party information does not include any information contained in a communication to which the target

~~SECRET~~

~~SECRET~~

is a party. The FBI shall limit, to the extent reasonably feasible, its acquisition of third-party information during the course of electronic surveillance or physical search. The foregoing does not preclude the acquisition of all information, communications, or data relating to the target in accordance with the applicable FISA authority where necessary to effect electronic surveillance or physical search of electronic data ~~(S)~~

III. RETENTION (U)**A. Retention — Storage of FISA-acquired Information. (U)**

The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with these and other applicable FBI procedures. These retention procedures apply to FISA-acquired information retained in any form. FBI electronic and data storage systems may permit multiple authorized users to access the information simultaneously or sequentially and to share FISA-acquired information between systems. "FISA-acquired information" means all information, communications, material, or property that the FBI acquires from electronic surveillance or physical search conducted pursuant to FISA. (U)

"Raw FISA-acquired information" is FISA-acquired information that (a) is in the same or substantially same format as when the FBI acquired it, or (b) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. Illustrative examples of raw FISA-acquired information include audio recordings of intercepted communications

~~SECRET~~

~~SECRET~~

(including copies thereof); soft or hard copies of e-mails and other Internet communications or data; digital images, negatives, or prints of photographs of documents obtained during a physical search; electronic storage media (including computer hard drives and removable storage media); verbatim translations of documents or communications; and intercepted communications that have been processed into the form of "tech cuts" but have not been evaluated to determine whether the tech cuts reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. ~~(S)~~

B. Retention – Access to FISA-acquired Information. (U)

The FBI may grant access to FISA-acquired information to all authorized personnel in accordance with policies established by the Director, FBI, in consultation with the Attorney General or a designee. The FBI's policies regarding access will vary according to whether a particular storage system contains raw FISA-acquired information, will be consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, and shall include provisions:

1. Permitting access to FISA-acquired information only by individuals who require access in order to perform their job duties or assist in a lawful and authorized governmental function;
2. Requiring the FBI to maintain accurate records of all persons to whom it has granted access;

~~SECRET~~

~~SECRET~~

3. Requiring the FBI to maintain accurate records of all persons who have accessed raw FISA-acquired information, and to audit its access records regularly to ensure that raw FISA-acquired information is only accessed by authorized individuals [REDACTED]

4. Requiring training on these minimization procedures and the FBI's policies regarding access to raw FISA-acquired information before granting access to raw FISA-acquired information; and

5. Requiring the primary case agent(s) and his/her/their designees (hereinafter "case coordinator(s)") to control the marking of information in a particular case in accordance with FBI policy. A marking, for example, would include an indication that the information is or is not foreign intelligence. ~~(S)~~

The FBI shall provide such policies to the Court when these procedures go into effect. Thereafter, the FBI shall provide any new policies or materially modified policies to the Court [REDACTED]

[REDACTED] ~~(S)~~

The FBI may make raw FISA-acquired information available to authorized personnel on a continuing basis for review, translation, analysis, and use in accordance with these procedures.

Authorized personnel may [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED]

[REDACTED] (S)

C. Retention – Review and Use of FISA-acquired Information. (U)

1. General Provisions. (U)

FBI personnel with authorized access to raw FISA-acquired information may review, translate, analyze, and use all such information only in accordance with these procedures and FISA and only for the purpose of determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. Such personnel shall exercise reasonable judgment in making such determinations. (S)

FBI personnel with authorized access may copy, transcribe, summarize, review, or analyze raw FISA-acquired information only as necessary to evaluate whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. Once FBI personnel have assessed that raw FISA-acquired information meets one of these criteria, the FBI may retain that information for further investigation and analysis and may disseminate it in accordance with these procedures. Pursuant to 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C), however, information that is assessed to be evidence of a crime but not to be foreign intelligence or necessary to understand foreign intelligence may only be retained and disseminated for law enforcement purposes. The FBI shall identify FISA-acquired information in its storage systems, [REDACTED] [REDACTED] that has been reviewed and meets these standards.

~~SECRET~~

~~SECRET~~

If the FBI proposes to use any storage system that is incapable of meeting these requirements, the FBI shall follow the procedures set forth in Section I.D. ~~(S)~~

Before using FISA-acquired information for further investigation, analysis, or dissemination, the FBI shall strike, or substitute a characterization for, information of or concerning a United States person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand or assess the importance of foreign intelligence information, or to be evidence of a crime. (U)

The FBI may disseminate copies, transcriptions, summaries, and other documents containing FISA-acquired information only in accordance with the dissemination procedures set forth in Part IV below. (U)

The FBI shall retain FISA-acquired information that is not foreign intelligence information that has been reviewed and reasonably appears to be exculpatory or impeachment material for a criminal proceeding, or reasonably appears to be discoverable in a criminal proceeding, and shall treat that information as if it were evidence of a crime. ~~(S)~~

2. Third-Party Information. (U)

The FBI may retain and use third-party information for investigative and analytical purposes in accordance with these procedures if such information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime (which is being retained or used for law enforcement purposes), and:

- (a) is a communication made or received on behalf of the target(s);

~~SECRET~~

~~SECRET~~

- (b) concerns activities in which the target(s) is or may be involved; or
- (c) concerns a serious threat of injury, loss of life, damage to property, or damage to the national security of the United States. ~~(S)~~

Third-party information that does not fall into these categories may be retained in accordance with Section III.G of these procedures but may not be used for investigation or analysis and may not be included in investigative or analytical documents such as Electronic Communications or reports. If, however, FBI personnel acquire information that does not fall into one of these categories but that they believe should be used, the FBI shall proceed in accordance with Sections I.D and I.E. ~~(S)~~

3. Categories of Non-Pertinent and Sensitive Information. (U)

FBI personnel shall continually analyze communications of or information concerning United States persons acquired pursuant to FISA for the purpose of establishing categories of information that are not foreign intelligence information, are not necessary to understand foreign intelligence information or assess its importance, or are not evidence of a crime. These categories should be established after a reasonable period of monitoring the communications of the target and shall be reported to the Court in a later renewal application relating to that target. When developing these categories, particular attention should be given to the following types of sensitive information:

(a) [REDACTED]

(b) [REDACTED]

[REDACTED]

~~SECRET~~

~~SECRET~~

(c) [REDACTED]

[REDACTED]

(d) [REDACTED]

(e) [REDACTED]

(f) [REDACTED]

(g) [REDACTED]

[REDACTED] ~~(S)~~

Before using information from an established category of sensitive information for investigation or analysis, including using the information in investigative or analytical documents such as Electronic Communications (ECs) or reports, FBI personnel shall determine that the information that falls into such categories reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

SECRET

~~SECRET~~

D. Retention — [REDACTED] (S)

Authorized users may query FBI electronic and data storage systems that contain raw FISA-acquired information to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. Such queries may involve the use of keywords, identifiers, formulas, attributes, or other sophisticated data exploitation techniques. To the extent reasonably feasible, authorized users must design such queries to find and extract foreign intelligence information or evidence of a crime and to minimize the extraction of third-party information. Authorized users may process the results of an appropriate query in accordance with Section III.C above. The FBI shall maintain records of all searches, including search terms, used to query such systems. (S)

Authorized users may query FBI electronic and data storage systems to find, extract, and analyze "metadata" pertaining to communications. The FBI may also use such metadata to analyze communications and may upload or transfer some or all such metadata to other FBI electronic and data storage systems for authorized foreign intelligence or law enforcement purposes. [REDACTED]

[REDACTED]

[REDACTED] (S)

~~SECRET~~

~~SECRET~~**E. Retention of Attorney-Client Communications. (U)**

This section governs the retention of attorney-client communications. In certain cases, however, the Government may propose and/or the FISC may order the use of supplemental procedures. FBI personnel shall consult as appropriate with FBI Division Counsel, the FBI Office of General Counsel, or the NSD to determine whether a communication is privileged. (U)

1. Target charged with a crime pursuant to the United States Code. (U)

As soon as the FBI knows that a target is charged with a crime pursuant to the United States Code, the FBI shall implement procedures that ensure that the target's attorney-client privilege is protected. These procedures shall include the following, unless otherwise authorized by the FISC:

a. Establishment of a review team of one or more monitors and/or reviewers, who have no role in the prosecution of the charged criminal matter, to initially access and review information or communications acquired from a surveillance or search of a target who is charged with a crime pursuant to the United States Code;

b. A procedure to ensure that as soon as the review team determines that the FBI has acquired a privileged communication concerning the charged criminal matter between the target and the attorney representing the target in that matter, the FBI will appropriately mark the communication privileged in a manner that is apparent to anyone who accesses the information, including in any FBI electronic and data storage system. An attorney representing the target in the criminal matter includes anyone working on behalf of that attorney, such as another attorney, an expert witness, a paralegal, or an administrative assistant; and

~~SECRET~~

~~SECRET~~

c. A procedure to ensure that within 10 business days of determining that a privileged communication under this section has been acquired [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Any electronic

versions of the privileged communications that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back-up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted privileged communications will not be accessible to any user and will be deleted from any restored system.

d. FISA-acquired information, other than privileged information that has been sealed according to Sections III.E.1.a-c, above, may subsequently be made available to the investigative team, including prosecutors, as appropriate.

e. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to a particular FISA search or surveillance, the FBI shall ensure that whenever any user reviews information or communications acquired from that search or surveillance, which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic notification that attorney-client communications have been acquired during the search or

~~SECRET~~

~~SECRET~~

surveillance. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications, (S).

2. Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States. (U)

FBI monitors and other personnel with access to FISA-acquired information shall be alert for communications that may be (i) between a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) between a person other than a target charged with a crime in the United States and the attorney representing the individual in the criminal matter. As soon as FBI personnel know that a target is charged with a non-Federal crime in the United States or someone other than the target who appears to regularly use the targeted facility, place, premises or property is charged with a crime in the United States, they will notify the Chief Division Counsel, FBI Office of General Counsel, and the NSD to determine whether supplemental procedures or a separate monitoring team are required. In the absence of such supplemental procedures or a separate monitoring team, as soon as FBI personnel recognize that they have acquired a communication between (i) a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) a person other than a target charged with a crime in the United States and the attorney representing the individual in the criminal matter, the FBI shall implement procedures that include the following:

- a. A procedure to ensure that the FBI immediately ceases monitoring or reviewing a privileged communication concerning the charged criminal matter;

~~SECRET~~

~~SECRET~~

b. [REDACTED]
[REDACTED]
[REDACTED]

c. A procedure to ensure that within 10 business days of determining that a privileged communication under this section has been acquired, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Any electronic versions of the privileged communications that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person except as permitted by the FISC. In the event FBI archival back up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted privileged communications will not be accessible to any user and will be deleted from any restored system; and

d. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to a particular FISA search or surveillance, the FBI shall ensure that whenever any user reviews information or communications acquired from that search or surveillance, which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic

~~SECRET~~

~~SECRET~~

notification that attorney-client communications have been acquired during the search or surveillance. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications. ~~(S)~~

3. Privileged communications involving targets and other persons not charged with a crime in the United States. (U)

The FBI may review and use FISA-acquired communications of a target or other person not charged with a crime in the United States that are attorney-client privileged in conducting a National Security investigation. Authorized FBI personnel who review FISA-acquired information that is privileged (i) must mark the communication (in hard copy and electronically) as privileged in a manner that is apparent to anyone who accesses the information; and (ii) may disseminate the item within the United States Intelligence Community if it otherwise meets the standards for dissemination. Before disseminating such item that otherwise meets the standards for dissemination outside the United States Intelligence Community, the FBI must obtain the approval of the Attorney General or the Attorney General's designee. ~~(S)~~

If the FBI determines that a privileged FISA-acquired communication of a person not charged with a crime in the United States is not foreign intelligence information but is evidence of a crime, the FBI must obtain approval to disseminate the information for law enforcement purposes from the Attorney General or the Assistant Attorney General for National Security. The FBI may disseminate the information immediately if it determines there is an immediate threat to life or of serious property damage. If the FBI makes such a dissemination, it shall immediately inform the NSD. ~~(S)~~

~~SECRET~~

~~SECRET~~

F. Additional Procedures for Retention, Use and Disclosure of FISA Information. (U)

1. Pursuant to 50 U.S.C. §§ 1806(b) and 1825(c), no information acquired pursuant to an order authorizing electronic surveillance or physical search under FISA shall be disclosed for law enforcement purposes unless [REDACTED]

[REDACTED] FISA-acquired information, including raw FISA-acquired information, may be disclosed for law enforcement purposes in criminal proceedings. ~~(S)~~

2. The FBI shall ensure that identities of any persons, including United States persons, that reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, [REDACTED] ~~(S)~~

3. Prosecutors. (U)

a. The FBI may disclose FISA-acquired information, including raw FISA-acquired information, and information derived therefrom, to federal prosecutors and others working at their direction, for all lawful foreign intelligence and law enforcement purposes, [REDACTED]

[REDACTED] When federal prosecutors and

~~SECRET~~

~~SECRET~~

others working at their direction are provided access to raw FISA-acquired information, they shall be trained on and comply with these and all other applicable minimization procedures. (S)

b. In accordance with applicable Attorney General-approved policies and procedures, federal prosecutors may also disclose FISA-acquired information, when necessary for the prosecutors to carry out their responsibilities, including to witnesses, targets or subjects of an investigation, or their respective counsel, when the FISA-acquired information could be foreign intelligence information or is evidence of a crime. This provision does not restrict a federal prosecutor's ability, in a criminal proceeding, to disclose FISA-acquired information that contains exculpatory or impeachment information or is otherwise discoverable under the Constitution or applicable federal law. (U)

c. The FBI may not provide federal prosecutors and others working at their direction [REDACTED] containing raw FISA-acquired information unless such access is: (a) for foreign intelligence or law enforcement purposes; (b) consistent with their responsibilities as federal prosecutors; and (c) pursuant to procedures established by the Attorney General and provided to the FISC. The procedures established by the Attorney General and provided to the FISC shall include the following:

- i. Access [REDACTED]
[REDACTED] must be limited to that which is consistent with their responsibilities as federal prosecutors and necessary to carry out their responsibilities efficiently during a specific investigation or prosecution;

~~SECRET~~

~~SECRET~~

- ii. Access must be requested from and approved by an executive at FBI Headquarters in a position no lower than Assistant Director (AD) and in coordination with the Deputy General Counsel of the FBI National Security Law Branch or a Senior Executive Service attorney in the National Security Law Branch, and will be considered on a case-by-case basis;
- iii. A request for access must specify [REDACTED], Foreign Intelligence Surveillance Court (FISC) docket numbers, and targeted facilities the prosecutor needs access, why such access is necessary, and the duration of such access;
- iv. All individuals receiving authorization to have direct access must receive [REDACTED] and training on the standard minimization procedures and any relevant supplemental minimization procedures applicable to the information to which they have access;
- v. Access shall be terminated no later than the conclusion of the relevant investigation or prosecution; and
- vi. Federal prosecutors may immediately be given access to FBI [REDACTED] raw FISA-acquired information if FBI personnel determine that an immediate

~~SECRET~~

~~SECRET~~

threat to life or of serious damage to property necessitates immediate access, and if such immediate access is given to federal prosecutors, notification shall be made to FBI Headquarters, FBI's Office of General Counsel, and NSD. ~~(S)~~

G. Time Limits for Retention. (U)

In general, the FBI may retain FISA-acquired information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. ~~(S)~~

1. The FBI is authorized to retain data in electronic and data [REDACTED]

[REDACTED], in accordance with the following:

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ~~(S)~~

b. [REDACTED]

[REDACTED] ~~(S)~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S)

2.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (S)

3. Audio and video recordings not accessible through an electronic and data storage system, and items and/or records obtained through physical search of premises or property, including images or copies of computer hard drives and removable media acquired during the execution of a physical search order, whether reviewed or not, but not identified as information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or evidence of a crime, shall be destroyed within specific time periods

~~SECRET~~

~~SECRET~~

as set forth in FBI policy, which shall provide for periodic destruction of certain categories of FISA-acquired information. This provision does not apply to FISA-acquired information within the scope of Section III.G.1 or III.G.2. ~~(S)~~

4. FISA-acquired information retained by the FBI in any other form. [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] ~~(S)~~

IV. DISSEMINATION (U)

A. Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies. (U)

The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information in accordance with Sections IV.A.1 and IV.A.2 to federal, state, local and tribal officials and agencies with responsibilities directly related to the information proposed to be disseminated. Information that reasonably appears to be foreign intelligence information not directly related to responsibilities of such agencies may be disseminated incidental to the dissemination of information directly related to responsibilities of such agencies. Such information may be disseminated only consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. (U)

1. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1). (U)

The FBI may disseminate to [REDACTED] FISA-acquired information concerning United States persons that reasonably appears to be necessary

~~SECRET~~

~~SECRET~~

to the ability of the United States to protect against: (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. ~~(S)~~

2. Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2). (U)

The FBI may disseminate to [REDACTED] FISA-acquired information concerning United States persons that reasonably appears to be necessary: (i) to the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States. Such information shall not be disseminated, however, in a manner that identifies a United States person, unless such person's identity is necessary to understand foreign intelligence information or to assess its importance. ~~(S)~~

B. Dissemination of Evidence of a Crime to Federal, State, Local and Tribal Officials. (U)

The FBI may disseminate, for a law enforcement purpose, FISA-acquired information concerning a United States person that reasonably appears to be evidence of a crime but not foreign intelligence information to [REDACTED]

[REDACTED] The FBI shall disseminate such FISA-acquired information in a manner consistent with the requirements of Section III.F. ~~(S)~~

~~SECRET~~

~~SECRET~~

C. Dissemination of Foreign Intelligence Information Concerning United States Persons to Foreign Governments. (U)

The FBI may disseminate FISA-acquired information concerning United States persons, which is foreign intelligence information, to foreign governments as follows:

1. Disseminations of FISA-acquired information concerning United States persons to the governments of the United Kingdom, Canada, Australia or New Zealand may be made upon the approval of the Director of the FBI, or a designee. ~~(S)~~
2. Disseminations of FISA-acquired information concerning United States persons to other foreign governments shall be made consistently with Department of Justice guidance and may be made upon the approval of the Director of the FBI, or a designee who shall hold a position no lower than Section Chief in the FBI, and shall be in coordination with the FBI Office of General Counsel, upon consideration of the following factors: the national security benefit the United States may reasonably expect to obtain from making the dissemination; the anticipated uses to which the foreign government will put the information; and any potential for economic injury, physical harm, or other restriction of movement to be reasonably expected from providing the information to the foreign government. If the proposed recipient(s) of the dissemination have a recent record of human rights abuses, that history should be considered in assessing the potential for economic injury, physical harm, or other restriction of movement, and whether the dissemination should be made. ~~(S)~~

Where there is a reasonable basis to anticipate that the dissemination will result in economic injury, physical harm, or other restriction of movement, no dissemination shall be

~~SECRET~~

~~SECRET~~

made without the approval of the Attorney General. If the Attorney General approves the dissemination, the FBI shall undertake reasonable steps to ensure that the disseminated information will be used in a manner consistent with United States laws, including Executive Order 12333 (as amended) and applicable federal criminal statutes. ~~(S)~~

3. The Attorney General, in consultation with the DNI or a designee, may authorize

[REDACTED]
[REDACTED]. Prior to granting such authorization, those officials shall consider, among other things: (1) whether such use is consistent with the national security interests of the United States, and (2) the effect of such use on any identifiable United States person. ~~(S)~~

4. The FBI will make a written record of each dissemination approved pursuant to this section, and information regarding such disseminations and approvals shall be [REDACTED]

[REDACTED] ~~(S)~~

D. [REDACTED]

~~(S)~~

The FBI may [REDACTED]

[REDACTED]
[REDACTED] Consistent with the other provisions of these procedures, the FBI is authorized to disseminate FISA-acquired information, including, tape recordings, transcripts, or electronic storage media (including computer hard drives and removable storage media), [REDACTED]

~~SECRET~~

~~SECRET~~

[REDACTED] The following restrictions apply with respect to any materials so disseminated:

1. Dissemination to [REDACTED]

[REDACTED] of such information or communications. [REDACTED]
[REDACTED]
[REDACTED] ~~(S)~~

2. Dissemination will be only to [REDACTED]

[REDACTED] of such information or communications. [REDACTED]
[REDACTED]
[REDACTED] ~~(S)~~

3. [REDACTED] shall make no permanent [REDACTED] record of information or communications of or concerning any person referred to in FISA-acquired information or recorded on FISA-acquired tape recordings, transcripts, electronic storage media (including computer hard drives and removable storage media), or other [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Records maintained [REDACTED] for this purpose may not be disseminated [REDACTED] [REDACTED]
[REDACTED] ~~(S)~~

4. Upon the conclusion [REDACTED] to the FBI, the FISA-acquired information, including all tape recordings, transcripts, electronic storage media (including

~~SECRET~~

~~SECRET~~

computer hard drives and removable storage media), or other items, or information disseminated

[REDACTED]

[REDACTED] (S)

5. Any information that [REDACTED] provide to the FBI as a result of [REDACTED] may be disseminated by the FBI in accordance with the applicable minimization procedures. (S)

E. [REDACTED] (S)

The FBI may disseminate [REDACTED]
[REDACTED] raw FISA-acquired information that relates to international terrorism acquired from electronic surveillance or physical search conducted by the FBI as provided in [REDACTED]

[REDACTED] (S)

F. [REDACTED] (S)

In addition to dissemination authorized under other provisions herein, foreign intelligence information, as defined in Section 1801(e), may be disseminated to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] (U)

~~SECRET~~

~~SECRET~~G. [REDACTED] ~~(S)~~

Notwithstanding any other provision of these procedures, the FBI may [REDACTED] [REDACTED] access to its [REDACTED] database, provided that such access is limited to classifications of cases that are likely to contain information [REDACTED] is contingent upon [REDACTED] [REDACTED] which are on file with the FISC. If the FBI authorizes [REDACTED] to disseminate any information [REDACTED] receives pursuant to this section, such authorization shall be made consistent with these procedures and applicable Department of Justice guidance, including but not limited to restrictions governing dissemination to foreign governments. ~~(S)~~

V, COMPLIANCE (U)

A. Oversight. (U)

To ensure compliance with these procedures, the Attorney General, through the Assistant Attorney General for National Security or other designee, shall implement policies and procedures that ensure the good faith compliance with all of the requirements set forth herein, and shall conduct periodic minimization reviews, including reviews at FBI Headquarters, field offices, and U.S. Attorney's Offices that receive raw FISA-acquired [REDACTED]

[REDACTED] The Attorney General and the NSD or other designee of the

~~SECRET~~

~~SECRET~~

Attorney General shall have access to all FISA-acquired information to facilitate minimization reviews and for all other lawful purposes. ~~(S)~~

To assess compliance with these procedures, minimization reviews shall consist of reviews of documents, communications, audit trails, or other information. They shall include, as appropriate, but are not limited to:

1. Reviews of electronic communications or other documents containing FISA-acquired information that have been retained for further investigation and analysis or disseminated in accordance with these procedures. ~~(S)~~
2. Reviews of FISA-acquired information (from electronic surveillance and physical search) in FBI electronic and data storage systems that contain raw FISA-acquired information to assess compliance with these procedures, including whether raw FISA-acquired communications or property have been properly marked as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. FISA-acquired communications and property in FBI electronic and data storage systems that contain raw FISA-acquired information may also be reviewed to determine whether they were properly marked pursuant to the attorney-client communications provisions of these procedures. ~~(S)~~
3. Audits of [REDACTED] raw FISA-acquired information to assess the FBI's compliance with the retention procedures for FISA-acquired information as detailed in Section III of these procedures. The audits may also include reviewing a sampling [REDACTED]

~~SECRET~~

~~SECRET~~

██████ and accesses in FBI electronic and data storage systems containing raw FISA-acquired information. These audits may assist in determining the FISA-acquired information that was accessed in these FBI electronic and data storage systems and the individuals who accessed the information. In turn, the minimization reviews may include verifying that the individuals who accessed the FISA-acquired information in these FBI systems were individuals who had properly been given access under FBI guidelines. (S)

B. Training. (U)

The Attorney General, or a designee, shall ensure that adequate training on these procedures be provided to appropriate personnel. (U)

C. Minimization Briefings. (U)

Following the authorization of collection activity, an NSD attorney shall conduct a minimization briefing with appropriate FBI personnel responsible for the FISA surveillance or search. (U)

VI. Interpretation (U)

The FBI shall refer all significant questions relating to the interpretation of these procedures to the NSD. (U)

~~SECRET~~

~~SECRET~~

VII. Review of Procedures (U)

The Attorney General, or a designee, in consultation with the FBI Office of General Counsel, shall review these procedures and determine whether they remain appropriate in light of the technology and practices used by the FBI no later than five years from the date of the Attorney General's approval of these procedures filed with the Court, and every five years thereafter. A written report of such review shall be provided to the Court within six months of the completion of the review. (U)



Michael B. Mukasey
Attorney General of the United States

10/22/08
Date

~~SECRET~~

EXHIBIT E

MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED ~~(S//NF)~~

With respect to unminimized communications the Central Intelligence Agency (CIA) receives from the National Security Agency (NSA) or the Federal Bureau of Investigation (FBI) that are acquired pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), the CIA will follow the following minimization procedures:

~~(S//NF)~~

1. Definitions:

- a. As used herein, the terms "Attorney General," "foreign power," "agent of a foreign power," "United States person," "person," "foreign intelligence information," "international terrorism," and "sabotage" have the meanings specified in sections 101 and 701 of the Act.
- b. The term "United States person identity" means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name or manufacturer's name, or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not a United States person identity. ~~(S//NF)~~

2. Unminimized communications acquired in accordance with section 702 of the Act and received by CIA will be maintained in access-controlled repositories that are accessible only to those who have had the required training and are physically or logically separated from repositories with general access. Unminimized communications that may contain United States person information that does not otherwise qualify for retention under paragraphs 3, 6, or 8 of these procedures may be retained in such access-controlled repositories for no longer than five years from the expiration date of the certification authorizing the collection unless the Director of the National Clandestine Service (NCS), or one of his or her superiors, determines that an extension is necessary because the communications are reasonably believed to contain significant foreign intelligence information, or evidence of a crime that has been, is being, or is about to be committed. An extension under this paragraph may apply to a specific category of communications, and must be documented in writing, renewed on an annual basis, and promptly reported to the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI). ~~(S//NF)~~

3. Information concerning a United States person may be retained by CIA indefinitely and outside of access-controlled repositories if (a) the information concerning the United States

~~SECRET//NOFORN~~

Classified by: The Attorney General
Reason: 1.4(c)
Declassify on: 11 April 2036

person is publicly available; (b) the United States person has consented to retention of the information concerning him or her; or (c) the United States person identity is deleted or otherwise sanitized to prevent the search, retrieval, or review of the identifying information (a generic term may be substituted which does not identify the United States person in the context of the data). If the information cannot be sanitized in such a fashion because the identity is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information, CIA may retain that information and the United States person identity indefinitely and outside of access-controlled repositories if: ~~(S//NF)~~

- a. The information is foreign intelligence information. Such information includes, but is not limited to, information falling within one or more of the following categories:
 - (1) the information indicates that the United States person has acted or may be acting as an agent of a foreign power, including information indicating that a United States person was in contact with a foreign power under facts and circumstances indicating that he intends to collaborate with a foreign power or become an agent of a foreign power;
 - (2) the information indicates that a United States person may be a target of intelligence activities of a foreign power;
 - (3) the information indicates that a United States person has engaged or may be engaging in the unauthorized disclosure of properly classified national security information; or
- b. The information concerns corporations or other commercial organizations the deletion of which would hamper the correlation of foreign intelligence information on the same subject;
- c. The information is enciphered or contains secret meaning;
- d. The information is needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of groups engaged in international terrorism;
- e. The information concerns a United States person who is or reasonably appears to be, on the basis of that or other information, an agent of a foreign power;
- f. The information indicates that a United States person is engaged or may be engaged in international terrorism or activities in preparation therefor;
- g. The information is needed and retained solely to identify individuals in contact with a foreign power or an agent of a foreign power (including for purposes of this subparagraph (g) any person, regardless of location, who engages in international terrorism or activities in preparation therefor; who aids, abets, or conspires with persons to engage in such activities; or who acts as a member of a group engaged in such activities);

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- h. [REDACTED]
- i. The information concerns a person or activity that poses a threat of sabotage, international terrorism, actual or potential attack or other grave hostile act, to any facility or personnel of any agency within the U.S. Intelligence Community, or any department containing such an agency;
- j. The information indicates that a United States person may be a target of intelligence activities of a foreign power; or
- k. The information concerns a U.S. Government official acting in an official capacity.
~~(S//NF)~~
4. CIA personnel may query CIA electronic and data storage systems containing unminimized communications acquired in accordance with Section 702 of the Act. [REDACTED]
[REDACTED] Such queries must be reasonably designed to find and extract foreign intelligence information. CIA will maintain records of all such queries, including but not limited to United States person names and identities, and NSD and ODNI will review CIA's activities that are conducted pursuant to this paragraph. ~~(S//NF)~~
5. Any information retained pursuant to paragraph 3 above may be disseminated to otherwise authorized recipients outside of CIA if the identity of the United States person and all personally identifiable information regarding the United States person are deleted or otherwise sanitized to prevent the search, retrieval or review of the identifying information. A generic term may be substituted which does not identify the United States person in the context of the data. However, if the information cannot be sanitized in such a manner because such person's identity is necessary to understand foreign intelligence information or assess its importance, that identity may be disseminated outside of CIA without such person's consent. Additionally, if the information cannot be sanitized in such a manner because it is reasonably believed that such person's identity may become necessary to understand or assess the importance of foreign intelligence information as defined by 50 U.S.C. § 1801 (e)(1), that identity may be disseminated outside of CIA without such person's consent.
~~(S//NF)~~
6. Nothing in these procedures shall prohibit:
- a. The retention or disclosure of information necessary for the purpose of determining whether the requirements of these procedures are satisfied, provided that the recipient under this paragraph does not retain or disclose the identity of a United States person where it is determined that the requirements of these procedures do not permit dissemination;

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

- b. The retention of communications necessary for the maintenance of technical data bases, so long as only collection or technical personnel have access to such data bases;
 - c. The retention or dissemination of information concerning corporations or other commercial organizations which is limited to their identities as manufacturers of equipment and related nomenclature or their locations;
 - d. The retention or dissemination of information required by law to be retained or disseminated; or
 - e. The retention or processing of communications in emergency data backup systems, provided that only administrative, collection, or technical personnel have access to such systems. In the event that information from such systems must be used to restore lost, destroyed, or inaccessible data, CIA shall apply these procedures to the transferred data.
(S//NF)
7. CIA will also follow the following procedures:

a.



- b. Dissemination to Foreign Governments: CIA may disseminate nonpublicly available identity or personally identifiable information concerning United States persons to foreign governments provided that such information is foreign intelligence information and either (i) the Attorney General approves the dissemination; or (ii) CIA disseminates the information under procedures that have been approved by the Attorney General. In addition, CIA may disseminate such foreign intelligence information acquired pursuant to Section 702 of the Act to the extent authorized by the Director of the CIA, and in

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

accordance with Director of National Intelligence Intelligence Community directives. CIA may make such disseminations without specific Attorney General approval subject to the following procedures:

[REDACTED]

- (3) Procedures for technical or linguistic assistance. It is anticipated that CIA may obtain from NSA and FBI unminimized information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments (collectively "assisting foreign governments") to assist CIA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, CIA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired by NSA or FBI pursuant to Section 702 of the Act to assisting foreign governments for further processing and analysis, provided that the following restrictions apply with respect to any materials so disseminated:
 - (a) Dissemination to assisting foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical assistance to CIA.
 - (b) Dissemination will be only to those personnel within assisting foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no further dissemination within assisting foreign governments of this raw data.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

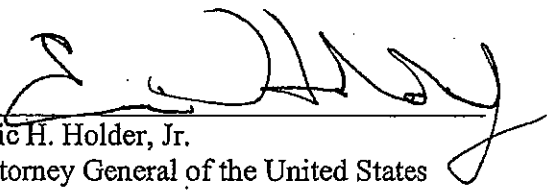
- (c) Assisting foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by CIA to assisting foreign government, provided that assisting foreign government may maintain such temporary records as are necessary to enable them to assist CIA with the translation or analysis of such information. Records maintained by assisting foreign governments for this purpose may not be disseminated within the assisting foreign government, except to personnel involved in providing technical assistance to CIA.
 - (d) Upon the conclusion of such technical assistance to CIA, computer disks, tape recordings, transcripts, or other items or information disseminated to assisting foreign government will either be returned to CIA or be destroyed with an accounting of such destruction made to CIA.
 - (e) Any information that assisting foreign governments provide to CIA as a result of such technical assistance may be disseminated by CIA in accordance with these minimization procedures.
- (4) CIA will make a written record of each dissemination approved pursuant to these procedures, and information regarding such disseminations and approvals will be made available for review by the Department of Justice. ~~(S//NF)~~
- c. Compliance With Crimes Reporting Obligations. Notwithstanding other provisions of these minimization procedures, information that is not foreign intelligence information, but reasonably appears to be evidence of a crime that has been, is being, or is about to be committed, may be retained and disseminated (including United States person identities) to the FBI and other appropriate federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. ~~(S//NF)~~
8. Any communication received by CIA that is acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or was in fact a United States person at the time of targeting will be destroyed unless the Director of the CIA specifically determines in writing that such communication is reasonably believed to contain significant foreign intelligence information or evidence of a crime that has been, is being, or is about to be committed. ~~(S//NF)~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

9. If CIA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life and that it is not feasible to obtain a timely modification of these procedures, CIA may take such action immediately. CIA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. ~~(S//NF)~~

9-17-11
Date


Eric H. Holder, Jr.
Attorney General of the United States

~~SECRET//NOFORN~~

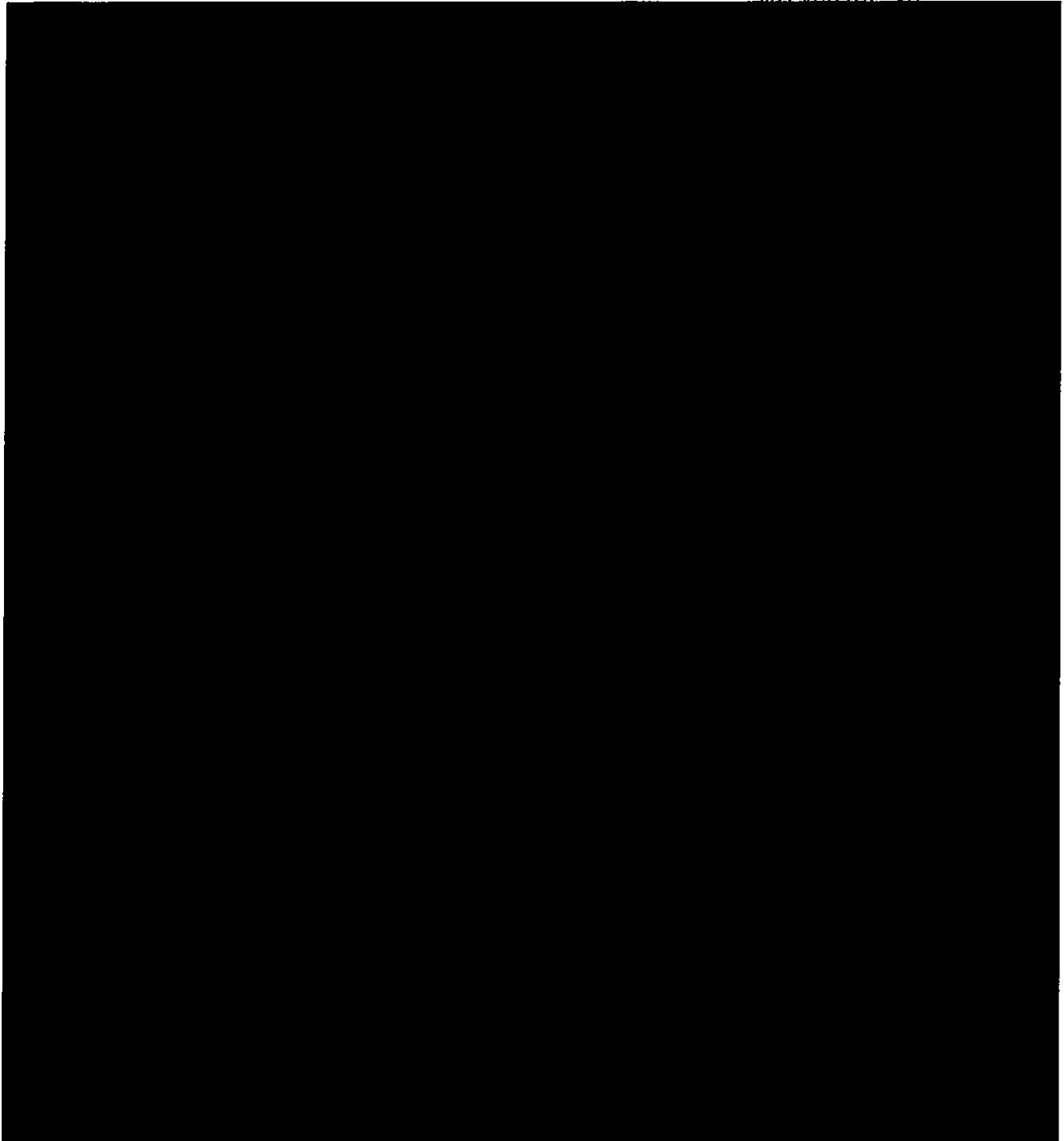
Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE ACT

EXHIBIT F



~~TOP SECRET//NOFORN~~

Derived From: NSA/CSSM 1-52

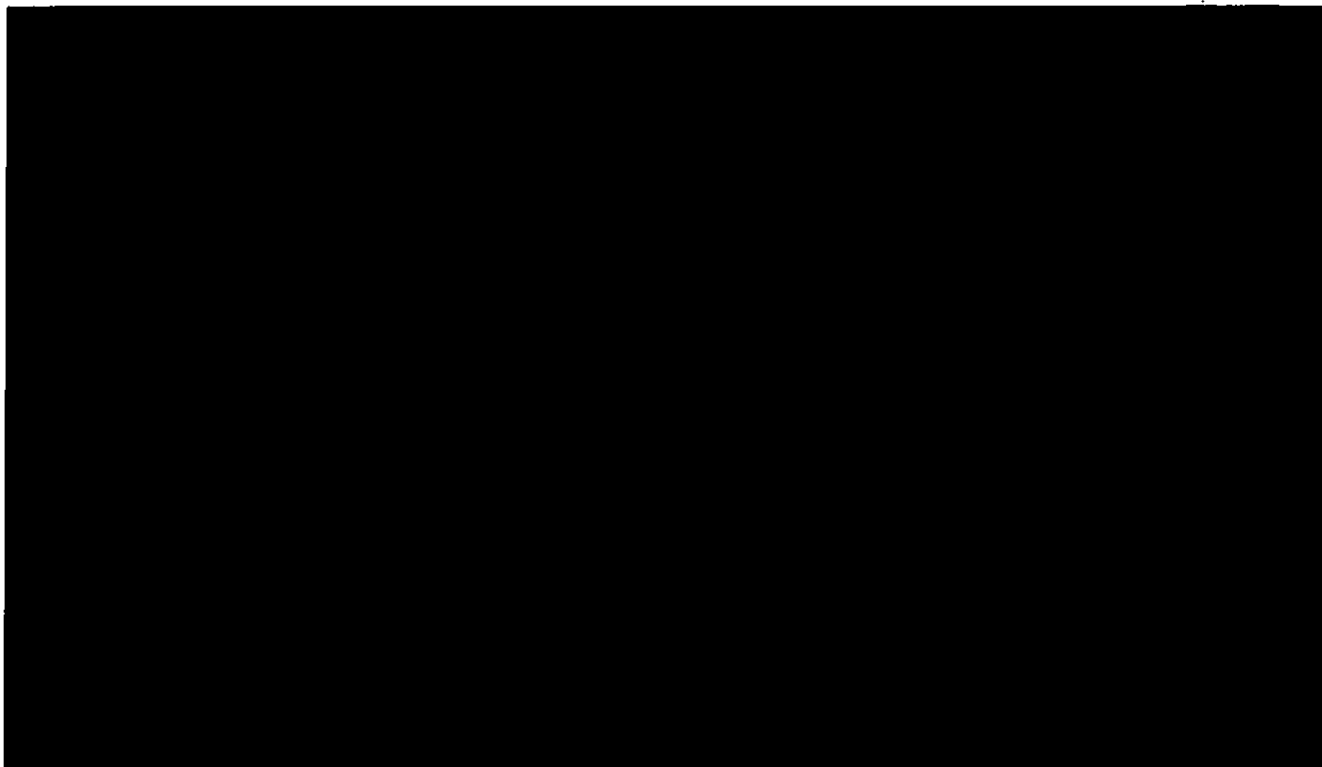
Dated: 20070108

Declassify On: 20340601

Approved for public release.

All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//NOFORN~~



~~TOP SECRET//NOFORN~~